目　　录

第一章 集　合

集合的概念是现代数学中最基本的概念之一，并已深入到各种科学和技术的领域中。对于计算机科学工作者来说，集合的概念是不可缺少的。在开关理论、有限自动机、形式语言等领域中，集合论有着广泛的应用。

这一章我们介绍集合及其子集、幂集、分划等基本概念，集合的并、交、补运算以及这些运算的性质；还介绍文氏图和成员表，它们是对集合进行运算和分析的有用工具；最后介绍集合的标准形式。

§1.1 集　合

集合是数学中的一个最基本的概念，很难再用别的词来定义它。我们通常只是给予一种描述。

把一些确定的、彼此不同的事物作为一个整体来考虑时，这个整体便称为是一个**集合**。这里所谓"事物"也称"个体"，可以是在极其广泛的意义上使用，甚至包括抽象的事物。例如，全体中国人，一本书中的全部概念，一群羊，所有自然数等等，都分别可以构成集合。

集合里所含有的个体叫做集合的**元素**。例如，全体中国人的集合，它的元素就是每一个中国人；一群羊的集合，它的元素就是该羊群中的每一只羊；所有自然数的集合，它的元素就是每一个自然数。

今后我们用大写拉丁字母表示集合，用小写拉丁字母表示元

素。如果 a 是集合 A 的元素，则记作"$a \in A$"，读作"a 属于集合 A"或"a 在集合 A 中"。如果 a 不是集合 A 的元素，则记作"$a \notin A$"，读作"a 不属于集合 A"或"a 不在集合 A 中"。例如，若用 N 表示自然数的集合，则 $2 \in N$，$3 \in N$，但 $2.3 \notin N$，$-5 \notin N$。

关于集合的概念，很重要的一点是当我们给出一个"个体"后，应该能够确定它是否是这个集合的元素。例如，"百货商店里好看的花布"就不成为一个集合，因为对每一种布，没有确定的标准说它是"好看"还是"不好看"。"这个班里的高个子学生"也不构成一个集合。因为在"高个子"与"不是高个子"之间没有明确的界限。但是，如果我们给出一个完全确定的标准（如身高 $h \geqslant 1.7$ 米），合乎这个标准的算是"高个子"，否则不算，那么对于这个班里的每一个学生，总可以明确地断定是否合乎这个标准，不会发生两可的情形，这时"这个班里的高个子学生"就构成一个集合。

下面介绍几个常见的集合的表示符号。

N：正整数或自然数集合$(1,2,3,\cdots)$。

Z：非负整数集合$(0,1,2,3,\cdots)$。

I：整数集合$(0,-1,1,-2,2,\cdots)$。

P：素数集合(只能被 1 和它本身整除，不能被其他正整数整除的大于 1 的正整数称作素数)。

Q：有理数集合(有理数是可以表示成 i/j 形式的数，这里 i 和 j 都是整数，且 $j \neq 0$)。

R：实数集合(包括全部有理数和无理数)。

C：复数集合(包括所有形如 $a+ib$ 的数，其中 a、b 是实数，$i=\sqrt{-1}$)。

$\mathbf{N}_m(m \geqslant 1)$：介于 1 和 m 之间的正整数集合，计入 1 和 m $(1,2,\cdots,m)$。

$\mathbf{Z}_m(m \geqslant 1)$：介于 0 和 $m-1$ 之间的非负整数集合，计入 0 和

$m-1(0,1,2,\cdots,m-1)$。

对于集合，有下面两种常用的表示方法。

把集合的元素按任意顺序逐一写在一个花括弧里，并用逗号分开，这称为**列举法**。例如，设 $a_1,a_2,\cdots,a_n$ 是集合 A 的元素，此外 A 无其它元素，则集合 A 可表示为 $A=\{a_1, a_2, \cdots, a_n\}$。又如，绝对值不超过 3 的所有整数的集合，可记作 $S=\{-3, -2, -1, 0,1,2,3\}$。列举法必须把元素的全体尽列出来，而不能遗漏任何一个，因此，如果一个集合含有许多元素时，用列举法是极其麻烦的。当集合含有无穷多个元素时，列举法更是无能为力。但对这种情形，有时也可列举出集合的一部分元素，而略掉的元素应能由列举出的元素以及它们前后的关系所确定，使得人们一看就明白。例如，$N=\{1,2,3,\cdots\}$，$I=\{\cdots-2,-1,0,1,2\cdots\}$。但这种写法有时是很困难的，可采用另一种表示方法。

集合的另一种表示法称为**描述法**，它是利用详细说明元素 $a\in A$ 的定义条件作出来的。即给定一个条件 $P(x)$，当且仅当 a 使条件 $P(a)$ 成立时，$a\in A$。其一般形式为 $A=\{a|P(a)\}$，读成"A 是使 $P(a)$ 成立的所有元素 a 的集合"。实际上，$P(a)$ 描述了一个规则或公式，它使得我们有可能确定 a 是否在 A 中。例如，绝对值不超过 3 的所有整数的集合用描述法可表示为 $S=\{a|a\in I$ 且 $-3\leqslant a\leqslant 3\}$。又如，$B=\{a|a$ 是中国的省$\}$。

用描述法来表示一个集合，其方式并不是唯一的，因为对一个集合的元素往往可以用多种不同的方式来确定。例如，集合 $\{1,2,3,4\}$ 的元素可定义为不大于 4 的自然数，也可定义为小于 6 而能整除12的自然数，因此集合 $\{1,2,3,4\}$ 可表示为 $\{a|a\in N, a\leqslant 4\}$，也可表示为 $\{a|a\in N, a<6, a|12\}$。

关于集合的概念，还有一点需要提起注意的是，对作为集合的元素的个体，并没有给它们施加什么限制。常常有一些集合其元素本身也是集合。例如，$A=\{5,\{1,2\},d,\{q\}\}$，$B=\{\{1\},\{2,3\},$

{1,3}}。对于这种情形，重要的是把集合 $\{a\}$ 与元素 a 区别开来。例如集合 $\{q\}$ 是集合 A 的元素，$\{q\}\in A$，而 q 是集合 $\{q\}$ 的元素，$q\in\{q\}$，但 q 不是 A 的元素，即 $q\notin A$。

然而，对"包罗一切的集合"或"由一切集合组成的集合"等类似的术语，我们必须避免使用，因为它们会导致集合论中的**悖论**。例如，我们来看著名的罗素悖论。

我们把不包含自身作为元素的集合称为寻常集，而把包含自身作为元素的集合称为不寻常集。于是可知，一个集合或者是寻常集，或者不是寻常集，二者必居其一，且只居其一。今设 T 是由所有寻常集组成的集合，即

$$T=\{A|A\text{是集合，}A\notin A\}.$$

现在我们考虑，T 是寻常集还是不寻常集？若 T 是寻常集，则由 T 的定义，T 必包含自身为元素，因此 T 是不寻常集。这与假设矛盾。故 T 不是寻常集，即 T 是不寻常集。然而由不寻常集的定义，就必须有 $T\in T$，因此 T 包含一个不寻常集为元素，这又与 T 的定义矛盾。这就是说，由于假定 T 的存在，无论 T 是寻常集或不寻常集都将引出矛盾。

又如，研究下述情况：某理发师跟且只跟城里所有不能给自己理发的人理发。定义 A 为城里所有由该理发师理发的人的集合，稍加考虑就会明白，A 一定是这样的集合，该理发师 $\in A$，而又有该理发师 $\notin A$。显然这是一个矛盾，因此集合 A 不存在。

定义 1-1 不含有任何元素的集合，称为**空集**，记作 ϕ。

空集看起来很不自然，但却是一个有用的概念。例如，我们说"两条平行线的交点之集是一个空集"即是说"两条平行线没有交点"。又如 $\{x|x\in I,x^2=8\}=\phi$，即意味着方程 $x^2=8$ 没有整数根。一般说来，如果我们想要证明命题 $P(x)$ 对于一切 x 均不真，则只要证明 $\{x|P(x)\}=\phi$ 即可。

集合 A 中不同元素的数目，称为集合 A 的**基数**，用 $\#A$ 表示。

当集合A具有有限数目的不同元素，亦即$\sharp A$为有限时，称A为**有限集**，否则称A为**无限集**。前述的集合$\boldsymbol{N},\boldsymbol{Z},\boldsymbol{I},\boldsymbol{P},\boldsymbol{Q},\boldsymbol{R}$和$\boldsymbol{C}$都是无限集；集合$\boldsymbol{N}_m$和$\boldsymbol{Z}_m$是有限集，因为$\sharp N_m=\sharp Z_m=m$。集合的基数后面还要较详细地讨论。

§1.2 集合的包含和相等

集合的包含和相等是集合间的两个基本关系。

定义 1-2 设有集合A、B，如果A的每一个元素都是B的元素（即若$a\in A$，必有$a\in B$），则称A是B的**子集**，或说A被包含于B中（或B包含A），记作$A\subseteq B$或$B\supseteq A$。反之，若A不是B的子集，则记作$A\nsubseteq B$或$B\nsupseteq A$。

例 1 设$A=\{a,c,d,e\}$，$B=\{a,b,c,x,y\}$，$C=\{a,b\}$，则有$C\subseteq B$，但$C\nsubseteq A$。

注意区别从属关系和包含关系。从属关系$a\in A$是指集合A的元素a与集合A的关系，而包含关系$C\subseteq A$是指集合A与另一个集合C之间的关系。

例 2 设$A=\{a,b,c,d\}$，则有$a\in A$，而$\{a\}\subseteq A$。

由从属关系和包含关系的定义可知，并不排斥同时有$A\in B$和$A\subseteq B$的可能性。

例 3 设$A=\{a,b,c\}$，$B=\{\{a,b,c\},a,b,c\}$，则显然有$A\in B$同时$A\subseteq B$。

关于集合的包含有如下重要性质：

(1) 对于任意的集合A，有$\phi\subseteq A$；

(2) 对于任意的集合A，有$A\subseteq A$；

(3) 对于任意的集合A、B、C，

若$A\subseteq B$，$B\subseteq C$，则有$A\subseteq C$。

性质（2）和（3）的成立是明显的。我们仅证明性质（1）。用

反证法，设空集 ϕ 不是某集合 A 的子集，即 $\phi \nsubseteq A$，则必存在元素 $x \in \phi$ 而 $x \notin A$，这与空集的定义矛盾，因此，$\phi \subseteq A$。

定义 1-3 设有集合 A、B，如果 A 的每一个元素都是 B 的元素，B 的每一个元素也都是 A 的元素，则集合 A 和 B 称为是**相等**，记作 $A = B$。

显然，所谓集合 A 与集合 B 相等，即意味着 A 与 B 具有完全相同的元素。

由定义 1-2 和定义 1-3 可知，当且仅当 $A \subseteq B$ 且 $B \subseteq A$ 时，有 $A = B$.

定义 1-3 的实质是一个集合由它的全部元素所确定。

下面给出一些相等集合和不等集合的例子.

例 4 $\{1,2,4\} = \{1,2,2,4\}$，

这就是说，在集合的第一种表示法中，某个元素的符号重复出现，不会改变这个集合。然而为了叙述的方便，今后我们不使用这种表示方法，要求列举的元素各不相同。

例 5 $\{1,4,2\} = \{1,2,4\}$，

这说明在集合的第一种表示法中，若将元素的次序任意改变，集合不变。

例 6 设 $P = \{\{1,2\},4\}$，$Q = \{1,2,4\}$，则 $P \neq Q$。

又 $\{\{1\}\} \neq \{1\}$。

如果 $A = \{x | x(x-1) = 0\}$，$B = \{0,1\}$，则 $A = B$。

定义 1-4 设有集合 A、B，若 $A \subseteq B$，且 $A \neq B$，则称集合 A 是集合 B 的**真子集**，用 $A \subset B$ 表示。

例如，集合 $\{1,2,3\}$ 是集合 $\{x | x \in I, -3 \leqslant x \leqslant 3\}$ 的真子集。

因为空集是每个集合的子集，所以导出如下定理。

定理 1-1 空集合是唯一的。

证明 假设有两个空集合 ϕ_1 和 ϕ_2，因为空集被包含于每一个集合中，因此有 $\phi_1 \subseteq \phi_2$，$\phi_2 \subseteq \phi_1$，这意味着 $\phi_1 = \phi_2$。证完。

§1.3 幂　集

任给一集合A，我们知道空集和集合A都是A的子集。对任何元素$a\in A$，集合$\{a\}$也是A的子集。类似地，我们还可以举出A的其它子集。下面我们来讨论关于集合A的全部子集的集合。

定义 1-5　设有集合A，由A的所有子集组成的集合，称为集合A的**幂集**，记作2^A，即

$$2^A=\{S\mid S\subseteq A\}.$$

例如，设$A=\{a\}$，则$2^A=\{\phi,\{a\}\}$；

$B=\{a,b\}$，则$2^B=\{\phi,\{a\},\{b\},\{a,b\}\}$；

$C=\{a,b,c\}$，则

$$2^C=\{\phi,\{a\},\{b\},\{c\},\{a,b\},\{a,c\},\{b,c\},\{a,b,c\}\}.$$

空集ϕ的幂集，仅含有元素ϕ，即$2^\phi=\{\phi\}$。

从上述例子可看出，当集合的基数增加时，集合的幂集的基数也随之增加。对于有限集下面的定理给出两者之间的关系。

定理 1-2　设A是具有基数$\#A$的有限集，则$\#(2^A)=2^{\#A}$。

证明　设$\#A=n$，从n个元素中选取i个不同元素的方法共有C_n^i种，这里

$$C_n^i=\frac{n!}{i!(n-i)!}.$$

所以A的不同子集的数目（包括ϕ）为

$$\#(2^A)=C_n^0+C_n^1+C_n^2+\cdots+C_n^n.$$

由二项式定理可知：

$$(x+y)^n=C_n^0x^n+C_n^1x^{n-1}y+C_n^2x^{n-2}y^2+\cdots+C_n^ny^n.$$

令$x=y=1$，便有

$$2^n=C_n^0+C_n^1+C_n^2+\cdots+C_n^n.$$

所以$\#(2^A)=2^n$。因为$\#A=n$，故有$\#(2^A)=2^{\#A}$。证完。

当集合A的元素个数较多时，要毫无遗漏地列出集合A的所有子集是一件相当困难的事情。现在我们引进一种表示法，按照这种表示法，我们能够毫无遗漏地列出一个有限集合的每一个子集。为此，我们对所给集合的元素规定某种次序，使得某个元素可以称为第一个元素，另一个元素为第二个元素，等等（虽然在集合的定义中，并没有这样一种次序），即给每一元素附加一个标号，以便描述这个元素相对于该集合其它元素的位置。例如，在集合$A=\{a,b,c\}$中，我们可以令a是第一个元素，b是第二个元素，c是第三个元素。在A的子集中，常常是有一些元素出现，而其余的元素不出现。我们根据这一情况以及指定给集合中各元素的次序，就用以下方式来表示所有的子集，例如A的各个子集可以表示为

$$B_{000}=\phi,\ B_{001}=\{c\},\ B_{010}=\{b\},\ B_{011}=\{b,c\},\ B_{100}=\{a\},$$
$$B_{101}=\{a,c\},\ B_{110}=\{a,b\},\ B_{111}=\{a,b,c\}.$$

因此 $$2^A=\{B_{000},B_{001},B_{010},B_{011},\cdots,B_{110},B_{111}\}.$$

其中，B的下标是一个三位的二进制数，每一位对应集合A中的一个元素，左边第一位是1还是0表示第一个元素a在子集中出现与否。类似地，第二位和第三位是1还是0分别表示第二个元素b和第三个元素c在子集中出现与否。于是，A的任一子集都可用000—111中的某一下标来表示，反之，若给出这8个（即2^3个）下标中的任何一个，就能够确定出相应的子集。

假设集合$J=\{j|j$是二进制数，$000\leqslant j\leqslant 111\}$，则有

$$2^A=\{B_j|j\in J\}.$$

可以看到，我们只用了下标来确定子集的各元素，而表示这些子集时用到的字母B则是无关紧要的。

上述表示法，可以推广到一般情形，用来表示具有任意n个不同元素的集合的各个子集。用来表示这些子集的下标是十进制数0到2^n-1的二进制表示。为了凑足n个数位，一定要在这些二

进制数的左边插入所需个数的零。我们也可以使用从 0 到 2^n-1 的十进制数来作为子集的下标，而只在要确定所对应子集的元素时才转换为二进制数。例如，令 $A_6=\{a_1,a_2,\cdots,a_6\}$，显然 A_6 有 $2^6=64$ 个子集。我们可称它们为 $B_0,B_1,\cdots,B_{2^6-1}$。下面我们看如何确定 A_6 的任何子集的各元素。

例　$B_7=B_{000111}=\{a_4,a_5,a_6\}$；

　　$B_{12}=B_{001100}=\{a_3,a_4\}$。

类似于集合的幂集，即所有元素都是集合的这种集合，我们今后还会经常遇到。我们称这种集合为**集合族**。例如，其和为 6 的不同正整数的集合的集合。

$$\{\{6\},\{1,5\},\{2,4\},\{1,2,3\}\}$$

就是一个集合族。

我们常用记号 $\{A_i\}_{i\in K}$ 来表示所有集合 $A_i(i\in K)$ 所构成的集合族，即

$$\{A_i\}_{i\in K}=\{A_i\mid i\in K\},$$

这里 K 是指标集。例如，集合族 $\{A_0, A_1, A_2, A_3, A_4\}$ 可表示为 $\{A_i\}_{i\in K}$，这里 $K=\{0,1,2,3,4\}$。当 $K=\{i\mid i\in I,\ i_1\leqslant i\leqslant i_2\}$ 时，又可将集合族 $\{A_i\}_{i\in K}$ 表示为 $\{A_i\}_{i=i_1}^{i_2}$。例如上一集合族又可表示为 $\{A_i\}_{i=0}^{4}$。

§1.4　集合的运算

我们再引进一个特殊的集合，它包含讨论中的每一个集合。

定义 1-6　如果一个集合包含了某个问题中所讨论的一切集合，则称它为该问题的全域集合，或简称为**全集合**，记作 U。

全集合 U 并非是唯一的，然而一般总是取一个较为方便取用的集合为 U。例如，若我们是在实数范围内讨论问题，则可将实数集 R 取作全集合 U；若在正整数范围内讨论问题，则可将正整

数集N取作全集合U。全集合U在问题讨论之初便取定，以后在讨论中涉及的每个集合均看作是全集合U的子集。

这一节，我们将讨论集合的几种运算，使用这些运算，通过对给定集合的元素进行组合，就能构成新的集合。

定义 1-7 设有集合A、B，属于A或属于B的所有元素组成的集合，称为A与B的**并集**，记作$A\cup B$，即

$$A\cup B=\{u\mid u\in A \text{ 或 } u\in B\}。$$

定义 1-8 设有集合A、B，属于A同时又属于B的所有元素组成的集合，称为A与B的**交集**，记作$A\cap B$，即

$$A\cap B=\{u\mid u\in A \text{ 且 } u\in B\}。$$

例 1 设 $A=\{a,b,c,d,e,f,g\}$；

$B=\{e,f,g,h,i\}$，

则

$$A\cup B=\{a,b,c,d,e,f,g,h,i\}；$$

$$A\cap B=\{e,f,g\}。$$

例 2 设$U=N$，$A=P$(素数集)，B为N中所有奇数的集合，则

$A\cup B$由所有正奇数和2组成；

$A\cap B$由除2以外的所有素数组成。

如果集合A与集合B没有公共元素，即$A\cap B=\phi$，则称A与B是**不相交**的。

例 3 设 $A_1=\{\{1,2\},\{3\}\}$，$A_2=\{\{1\},\{2,3\}\}$，

$A_3=\{\{1,2,3\}\}$，

则$A_1\cap A_2=\phi$，$A_1\cap A_3=\phi$，$A_2\cap A_3=\phi$。所以集合A_1、A_2和A_3两两互不相交。

由上述定义，显然可以得到以下关系式：

$$A\subseteq A\cup B, \qquad B\subseteq A\cup B;$$

$$A\cap B\subseteq A, \qquad A\cap B\subseteq B。$$

如果 $A\subseteq B$，则 $A\cup B=B$，$A\cap B=A$。

定义 1-9　设有集合A、B，由属于B而不属于A的所有元素组成的集合，称为A关于B的**相对补集**，记作$B-A$，即

$$B-A=\{u \mid u\in B,\ u\notin A\}。$$

A关于B的相对补集，也称为B与A的差集。

例 4　设 $A=\{2,5,6\}$，　　$B=\{3,4,2\}$，

则

$$B-A=\{3,4\},\qquad A-B=\{5,6\}。$$

一个特别重要的情况，是集合A关于全集合U的相对补集。

定义 1-10　集合A关于全集合U的相对补集，称为A的绝对补集，简称为A的**补集**，记作A'，即

$$A'=U-A=\{u \mid u\in U,\ u\notin A\}=\{u \mid u\notin A\}。$$

例 5　设$U=Z$，$A=\{2k \mid k\in Z\}$，

则

$$A'=\{2k+1 \mid k\in Z\}\text{是所有正奇数的集合。}$$

显然$U'=\phi$，$\phi'=U$。

假设$\{A_i\}_{i=1}^{n}$是全集合U中的一组子集，我们把对ϕ、U、A_1，A_2、…、A_n任意施加$'$、$\cup$、$\cap$运算有限次所产生的集合，称为由A_1，A_2，…，A_n所产生的集合。例如ϕ，$B\cap C'$，$((A\cup B')\cap C)'\cup A'$和$U$都是由$A,B,C$所产生的集合。

§1.5　文氏图

全集的引进，使得我们能够利用图示的方法来研究全集中各子集之间的关系，以及它们的并、交、补等运算。所用的图称为**文氏图**(John Venn，英国数学家，1834—1883)。文氏图是用点的集合作为一个集合的示意表示。在文氏图中全集U用一长方形区域表示，长方形中的点表示全集U中的元素。U的子集用该长方形内的圆形区域表示。图 1-1 中的阴影区域表示了每个图形下边所指出的集合。

由图 1-1 的这些文氏图容易看出下列关系是成立的：

$$A\cup B=B\cup A,\qquad A\cap B=B\cap A,\qquad (A')'=A.$$

而且，如果 $A\subseteq B$，则 $A-B=\phi$，$A\cap B=A$ 和 $A\cup B=B$。

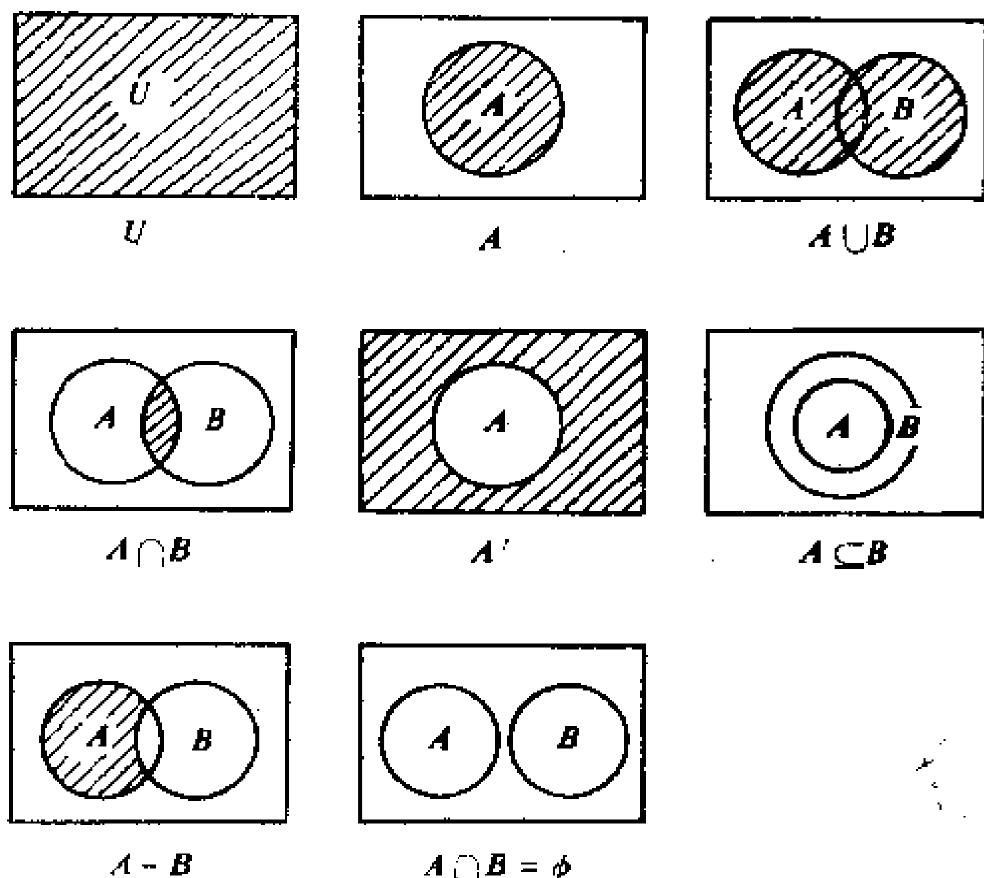


图 1-1

由图 1-2 表示的文氏图可方便地得到 U 的两个子集 A 和 B 的许多关系。这两个子集分 U 为四个互不相交的子集，它们在图中用区域 S_1，S_2，S_3，S_4 表示。由图显然有

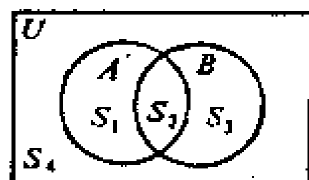


图 1-2

$$A-B=A\cap B'.$$

因为 $\qquad A-B=S_1,$

$$A\cap B'=(S_1\cup S_2)\cap(S_1\cup S_4)=S_1.$$

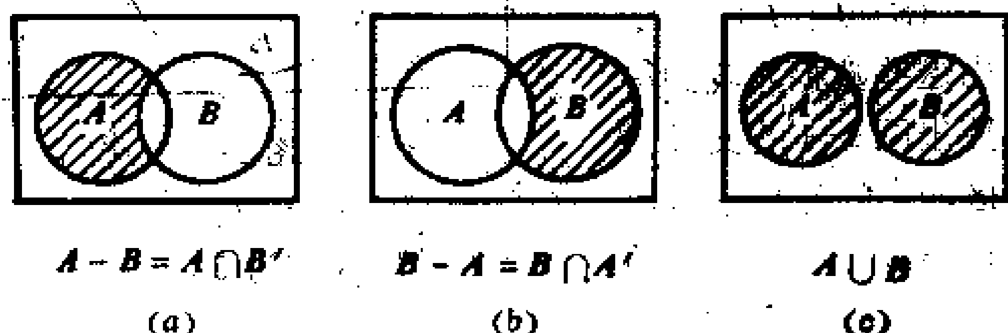
又有等式 $\quad (A\cup B)'=A'\cap B',$

因为 $$(A\cup B)'=(S_1\cup S_2\cup S_3)'=S_4,$$

$$A'\cap B'=(S_3\cup S_4)\cap(S_1\cup S_4)=S_4.$$

应该指出，文氏图只是起一种示意的作用，它可启示出子集之间的某些关系。但利用文氏图来证明集合恒等式，一般来说是不太合适的。特别当集合的数目增多时，文氏图将要得很复杂。而且，有些文氏图不能用来证明对于U中所有子集普遍成立的关系。

例如，我们看图 1-3 中的文氏图。



$A-B=A\cap B'$ (a)　　$B-A=B\cap A'$ (b)　　$A\cup B$ (c)

图 1-3

由 (a)、(b) 可以看出：

$$A\cup B=(A\cap B')\cup(B\cap A')\cup(A\cap B). \quad (1)$$

但由 (c) 得到：

$$A\cup B=(A\cap B')\cup(B\cap A'). \quad (2)$$

(2) 式虽然对 $A\cap B=\phi$ 这一特定情况来说是正确的，但在一般情况下，它是不正确的。

下面的例子说明，使用文氏图能够简单、直观地解决一些复杂的问题。

例 在一个 170 人的班级里，120 个学生会西班牙语；80 个个学生会法语；60个学生会英语；50个学生既会西班牙语又会法语；25个学生既会西班牙语又会英语；30个学生既会法语又会英语；10个学生三种语言全都会，问有多少学生对这三种语言一种也不会？

解 分别用 S,F,E 表示会西班牙语，法语，英语的学生的集

合，于是

$\#S=120$，

$\#F=80$，

$\#E=60$，

$\#(S\cap F)=50$，

$\#(S\cap E)=25$，

$\#(F\cap E)=30$，

$\#(S\cap F\cap E)=10$。

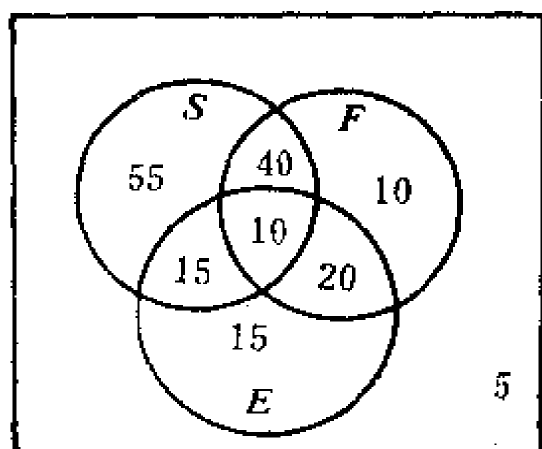


图 1-4

由这些数据，我们可以计算出图 1-4 的文氏图各个区域中的元素个数，因而得出对三种语言一种也不会的学生人数为 5。

§1.6 集合成员表

前面定义了集合的并、交、补等运算。不难理解，所有这些对全集U的子集进行的运算对全集U是封闭的，即由这些运算所产生的新的集合仍为全集U的子集。下面，我们对上述集合的基本运算作出另外一种形式的定义。

集合 A 的补集，可如下定义：

若 $u\notin A$，则 $u\in A'$；

若 $u\in A$，则 $u\notin A'$。

集合 A 和 B 的并集，可如下定义：

若 $u\notin A$，$u\notin B$，则 $u\notin A\cup B$；

若 $u\notin A$，$u\in B$，则 $u\in A\cup B$；

若 $u\in A$，$u\notin B$，则 $u\in A\cup B$；

若 $u\in A$，$u\in B$，则 $u\in A\cup B$。

集合 A 和 B 的交集，可如下定义：

若 $u\notin A$，$u\notin B$，则 $u\notin A\cap B$；

若 $u\notin A$，$u\in B$，则 $u\notin A\cap B$；

若 $u\in A$，$u\notin B$，则 $u\notin A\cap B$；

若 $u\in A$，$u\in B$，则 $u\in A\cap B$。

可以把这些定义加以概括，列举在表1-1所示的**成员表**中。表中标有集合 S 的列中的数字0和1分别表示元素 $u\notin S$ 和 $u\in S$。

表 1-1

(a) A' 的成员表

A	A'
0	1
1	0

(b) $A\cup B$ 的成员表

A	B	$A\cup B$
0	0	0
0	1	1
1	0	1
1	1	1

(c) $A\cap B$ 的成员表

A	B	$A\cap B$
0	0	0
0	1	0
1	0	0
1	1	1

A 和 B 所产生的集合的成员表，可推广到任意子集 A_1，A_2，…，A_r 所产生的集合上去。一般地，对于 $A_1, A_2, \cdots, A_r$ 所产生的集合 S 的成员表，其前 r 列标记 $A_1, A_2, \cdots, A_r$，最后一列标记 S，标记 A_i 的列中数字0表示 $u\notin A_i$，数字1表示 $u\in A_i$。若在第 k 行上，前 r 列所指明的条件下有 $u\notin S$，则在 S 列的第 k 行位置上记入0，否则，即若有 $u\in S$，则记入1。成员表共有 2^r 行，它相应于 u 在 $A_1, A_2, \cdots, A_r$ 中的 2^r 种可能的**成员/非成员情况**。为简化讨论，有时把标记 $A_1, A_2, \cdots, A_r$ 列中的一行数字 $\delta_1\delta_2\cdots\delta_r$（其中每个 δ_i 取0或1）称为行 $\delta_1\delta_2\cdots\delta_r$。

例如，表1-2说明由 A，B，C 所产生的集合

$$S=((A\cap B)\cup(A'\cap C))\cup(B\cap C)$$

的成员表的构造。

在表1-2中前3列列出了 u 在 A、B、C 中的8种可能的成员/非成员情况，而最后一列列出了 u 在 S 中的相应成员/非成员情况。这一列是通过集合 A'、$A\cap B$、$A'\cap C$、$B\cap C$ 和 $(A\cap B)\cup$

$(A'\cap C)$的中间成员表相继构造出来的。除前三列外，每一列都是由前面的列直接参照′、∪、∩的成员表构造出来的。

表1-2　$((A\cap B)\cup(A'\cap C))\cup(B\cap C)$的成员表

A	B	C	A′	A∩B	A′∩C	B∩C	(A∩B)∪(A′∩C)	((A∩B)∪(A′∩C))∪(B∩C)
0	0	0	1	0	0	0	0	0
0	0	1	1	0	1	0	1	1
0	1	0	1	0	0	0	0	0
0	1	1	1	0	1	1	1	1
1	0	0	0	0	0	0	0	0
1	0	1	0	0	0	0	0	0
1	1	0	0	1	0	0	1	1
1	1	1	0	1	0	1	1	1

在成员表中，若某列的各记入值全为0，则该列所标记的集合是空集Φ；反之，若全为1，则该列所标记的集合是全集合U。如果成员表中标有S和T的两列是恒同的(即S和T的列中任何一行的记入值都相等)，则$u\in S$蕴涵$u\in T$，同时$u\in T$蕴涵$u\in S$，所以$S=T$。例如，在表1-2中$(A\cap B)\cup(A'\cap C)$与$((A\cap B)\cup(A'\cap C))\cup(B\cap C)$的列是完全一样的，因此有

$$(A\cap B)\cup(A'\cap C)=((A\cap B)\cup(A'\cap C))\cup(B\cap C),$$

于是，成员表可以用来证明由全集合U的子集所产生的集合是否相等。

§1.7　集合运算的定律

集合的并、交、补运算具有许多性质，在§1.5中我们已初步看到了一些。下面列出这些性质中最主要的几条，并称它们为集合运算的基本定律。

对于全集合U的任意子集A、B、C，有：

交换律 1. $A\cup B=B\cup A$；　　1′. $A\cap B=B\cap A$。

结合律 2. $A\cup(B\cup C)=(A\cup B)\cup C$；

2′. $A\cap(B\cap C)=(A\cap B)\cap C$。

分配律 3. $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$，

3′. $A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$。

同一律 4. $A\cup\phi=A$；　　4′. $A\cap U=A$。

互补律 5. $A\cup A'=U$；　　5′. $A\cap A'=\phi$。

此外，集合运算的下述定律也是经常用到的：

对合律 6.6′. $(A')'=A$。

等幂律 7. $A\cup A=A$；　　7′. $A\cap A=A$。

零一律 8. $A\cup U=U$；　　8′. $A\cap\phi=\phi$。

吸收律 9. $A\cup(A\cap B)=A$；　9′. $A\cap(A\cup B)=A$。

德·摩根律 10. $(A\cup B)'=A'\cap B'$；

10′. $(A\cap B)'=A'\cup B'$.

由于以上各等式对于U的任意子集A、B和C都是成立的，因此它们是集合恒等式。这些集合恒等式的正确性，我们均可以一一加以证明。下面举例说明这些集合恒等式的证明方法。

根据定义进行证明。

例1 德·摩根定律 $(A\cup B)'=A'\cap B'$

证明 设$u\in(A\cup B)'$，则$u\notin A\cup B$，因而$u\notin A$且$u\notin B$，于是$u\in A'$且$u\in B'$，从而$u\in A'\cap B'$，故有$(A\cup B)'\subseteq A'\cap B'$。

反之，设$u\in A'\cap B'$，则$u\in A'$且$u\in B'$，于是$u\notin A$且$u\notin B$，因而$u\notin A\cup B$，有$u\in(A\cup B)'$，故有$A'\cap B'\subseteq(A\cup B)'$。

由上可知$(A\cup B)'=A'\cap B'$。

用列集合成员表的方法进行证明。

例2 结合律 $A\cup(B\cup C)=(A\cup B)\cup C$

证明 列出集合$A\cup(B\cup C)$和$(A\cup B)\cup C$的成员表如下：

A	B	C	$B\cup C$	$A\cup B$	$A\cup(B\cup C)$	$(A\cup B)\cup C$
0	0	0	0	0	0	0
0	0	1	1	0	1	1
0	1	0	1	1	1	1
0	1	1	1	1	1	1
1	0	0	0	1	1	1
1	0	1	1	1	1	1
1	1	0	1	1	1	1
1	1	1	1	1	1	1

因为成员表中集合 $A\cup(B\cup C)$ 与 $(A\cup B)\cup C$ 所标记的列完全相同，所以 $A\cup(B\cup C)=(A\cup B)\cup C$。

所有的集合恒等式都可用以上两方法类似地加以证明。

以上所列举的集合恒等式不全都是独立的，如果我们证明了一些恒等式是正确的，那么就可以利用它们来证明另外的一些恒等式。

例 3 假设交换律、分配律、同一律和零一律都是正确的，我们来证明吸收律

$$A\cup(A\cap B)=A.$$

证明 $A\cup(A\cap B)=(A\cap U)\cup(A\cap B)$ （由同一律）

$=A\cap(U\cup B)$ （由分配律）

$=A\cap(B\cup U)$ （由交换律）

$=A\cap U$ （由零一律）

$=A.$ （由同一律）

结合律指出，对任何的集合 A、B、C，有 $A\cup(B\cup C)=(A\cup B)\cup C$ 以及 $A\cap(B\cap C)=(A\cap B)\cap C$。因此，我们常删去括号而将其分别写作 $A\cup B\cup C$ 和 $A\cap B\cap C$。用归纳法容易证明，对于任意 n 个集合 $A_1, A_2, \cdots, A_n$，它们的并与交也是满足结合律的，因此对其表达式也可以不加括号而写成

$$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \cdots \cup A_n = \{u \mid u \in A_1 \text{或} u \in A_2 \cdots \text{或} u \in A_n\};$$

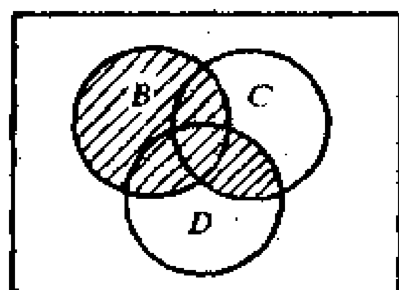
$$\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \cdots \cap A_n = \{u \mid u \in A_1, u \in A_2, \cdots, u \in A_n\}.$$

类似地，分配律也可以推广到一般情形：

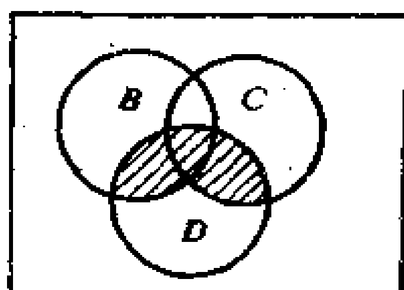
$$B \cap (\bigcup_{i=1}^{n} A_i) = \bigcup_{i=1}^{n} (B \cap A_i);$$

$$B \cup (\bigcap_{i=1}^{n} A_i) = \bigcap_{i=1}^{n} (B \cup A_i).$$

当连续进行并与交的运算时，为了避免含混，必须使用括号。和算术运算一样，总是约定从最内层的括号内的运算作起。例如在 $A = B \cup (C \cap D)$ 中，括号就规定了 A 由如下运算次序而得到：(1) 先求 C 与 D 的交集 E。(2) 再求 B 与 E 的并集。其结果与 $(B \cup C) \cap D$ 是完全不同的。因此无括号的式子 $B \cup C \cap D$ 是含混的。下面以图1-5的阴影部分加以说明。



$B \cup (C \cap D)$



$(B \cup C) \cap D$

图1-5

§1.8 分　划

定义1-11 设 $\pi = \{A_i\}_{i \in K}$ 是集合 A 的某些非空子集的集合。如果集合 A 的每一元素在且只在其中之一 A_i 中，即如果

(1) $A_i \cap A_j = \phi$，当 $i \neq j$ 时；

(2) $\bigcup_{i \in K} A_i = A$，

则称集合 π 是集合 A 的一个**分划**. 每个 A_i 称为这个分划的一个**分划块**。

图1-2中的集合 $\{S_1, S_2, S_3, S_4\}$ 就是 U 的一个分划。

例 1 设 $A = \{1,2,3\}$,

则 $\pi_1 = \{\{1\},\{2\},\{3\}\}$, $\pi_2 = \{\{1\},\{2,3\}\}$,

$\pi_3 = \{\{2\},\{1,3\}\}$, $\pi_4 = \{\{3\},\{1,2\}\}$, $\pi_5 = \{\{1,2,3\}\}$

都是 A 的分划. 由此可知, 一个集合的分划, 一般来说不是唯一的。

例 2 设 $A = I$。A_i 是 A 中被 5 除后余数为 i(参见§3.8)的所有整数的集合. 则

$$A_0 = \{\cdots, -10, -5, 0, 5, 10, \cdots\};$$
$$A_1 = \{\cdots, -9, -4, 1, 6, 11, \cdots\};$$
$$A_2 = \{\cdots, -8, -3, 2, 7, 12, \cdots\};$$
$$A_3 = \{\cdots, -7, -2, 3, 8, 13, \cdots\};$$
$$A_4 = \{\cdots, -6, -1, 4, 9, 14, \cdots\}.$$

因为任何一个整数被 5 除后的余数 i 是唯一的, 并且满足 $0 \leq i < 5$, 所以集合 I 中的每一个整数在且只在上述五个集合之一中。于是集合 $\{A_0, A_1, A_2, A_3, A_4\}$ 是整数集 I 的一个分划。

相应于子集和真子集的概念, 分划中给出了细分和真细分的概念。

定义 1-12 设 $\bar{\pi} = \{\bar{A}_i\}_{i \in \bar{K}}$ 和 $\pi = \{A_j\}_{j \in K}$ 都是集合 A 的分划, 如果 $\bar{\pi}$ 中的每一个 $\bar{A}_i$ 都是 π 中某个 A_j 的子集, 则称分划 $\bar{\pi}$ 是分划 π 的一个**细分**。如果 $\bar{\pi}$ 是 π 的细分, 且 $\bar{\pi}$ 中至少有一个 $\bar{A}_i$ 为某个 A_j 的真子集, 则称 $\bar{\pi}$ 是 π 的**真细分**。

例如, 例 1 中的 π_1 是 π_2、π_3、π_4 和 π_5 的细分, 也是它们的真细分。π_2、π_3、π_4 都是 π_5 的真细分。显然, 每个 π_i 都是自己的细分, 但不是真细分。

在文氏图上, 分划全集 U 的过程, 可看作是在表示 U 的区域

上划出分界线。如果分划$\bar{\pi}$的分界线是在分划π已有的分界线上至少加上了一根新的分界线所组成，则$\bar{\pi}$就是π的真细分。

§1.9 集合的标准形式

（一） 最小集标准形式

定义1-13 设$A_1,A_2,\cdots,A_r$是全集合U的子集，形为$\bigcap_{i=1}^{r}\overline{A}_i$的集合称为由$A_1,A_2,\cdots,A_r$所产生的**最小集**，其中每个$\overline{A}_i$为$A_i$或$A_i'$。

例如，由集合A，B，C所产生的全部最小集是：$A\cap B\cap C$、$A\cap B\cap C'$、$A\cap B'\cap C$、$A\cap B'\cap C'$、$A'\cap B\cap C$、$A'\cap B\cap C'$、$A'\cap B'\cap C$、$A'\cap B'\cap C'$。

显然，由$A_1,A_2,\cdots,A_r$所产生的最小集共有2^r个。

图1-6所显示的情形是，由A,B,C所产生的8个最小集都不为空集。图1-7所显示的情形是。

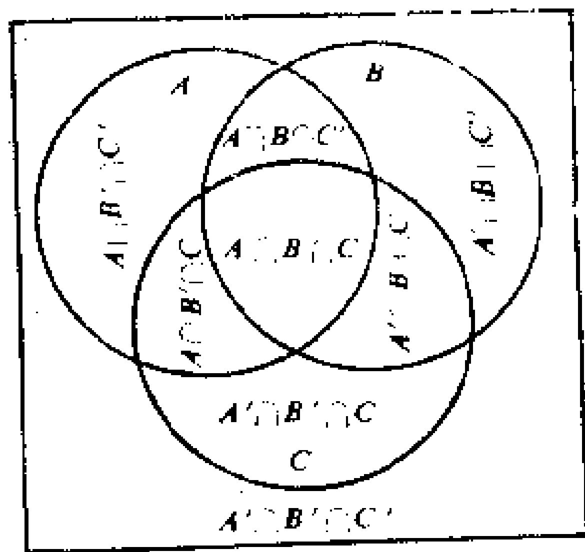


图1-6

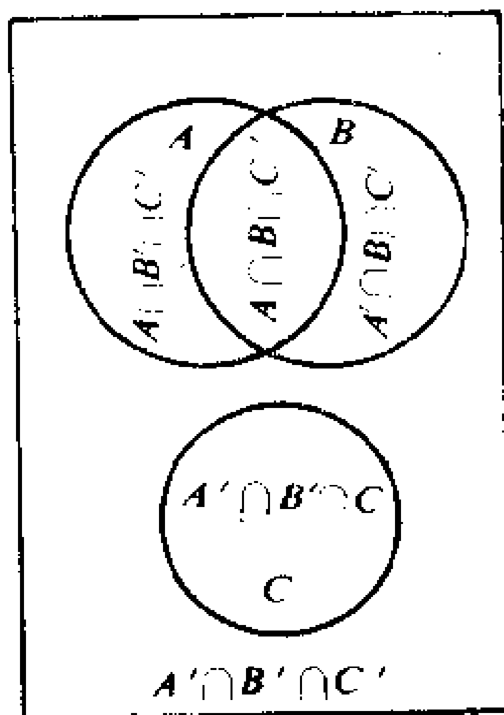


图1-7

在 A, B, C 所产生的最小集中

$$A\cap B\cap C=A\cap B'\cap C=A'\cap B\cap C=\phi.$$

定理 1-3 由 $A_1,A_2,\cdots,A_r$所产生的所有非空最小集的集合构成U的一个分划。

图1-6与图1-7已初步显示了定理1-3所述的结论，下面给出定理的一般证明。

证明 设任一元素$u\in U$，则$u\in A_1$，或者$u\in A_1'$；$u\in A_2$，或者$u\in A_2'$；…；$u\in A_r$，或者$u\in A_r'$。因此u必在某个最小集$\bigcap\limits_{i=1}^{r}\overline{A}_i$中。

又设有某一元素$u\in U$，使得$u\in S_1\cap S_2$，其中S_1和S_2是A_1，$A_2,\cdots,A_r$产生的两个不同的最小集，则必存在一个$i(1\leqslant i\leqslant r)$，使得$u\in A_i$同时$u\in A_i'$，但$A_i\cap A_i'=\phi$，因此$u\in S_1\cap S_2$是不可能的，即$U$中任一元素只能在一个最小集中．证完。

为了方便，我们用$M_{\delta_1\delta_2\cdots\delta_r}$来表示最小集$\overline{A}_1\cap\overline{A}_2\cap\cdots\cap\overline{A}_r$，其中

$$\delta_i=\begin{cases}0 & \text{当 } \overline{A}_i=A_i'; \\ 1 & \text{当 } \overline{A}_i=A_i.\end{cases}$$

例如，$A_1\cap A_2\cap A_3'\cap A_4$表示为$M_{1101}$，$A_1'\cap A_2'\cap A_3\cap A_4$表示为$M_{0011}$。这样$M_{\delta_1\delta_2\cdots\delta_r}$的下标使唯一地描述了所要表示的最小集。

考察任意一个最小集$M_{\delta_1\delta_2\cdots\delta_r}=\bigcap\limits_{i=1}^{r}\overline{A}_i$和它的成员表。按交集的定义，当且仅当$u\in\overline{A}_1$，$u\in\overline{A}_2$，…，$u\in\overline{A}_r$时，$u\in M_{\delta_1\delta_2\cdots\delta_r}$。因此，在$M_{\delta_1\delta_2\cdots\delta_r}$所标记的列中，有一个且仅有一个1。该1出现的行就是$\overline{A}_1$，$\overline{A}_2$，…，$\overline{A}_r$所标记的各列处均为1的行，也就是A_1，$A_2,\cdots,A_r$所标记的各列处分别为$\delta_1,\delta_2,\cdots,\delta_r$的行。这就是说，$M_{\delta_1\delta_2\cdots\delta_r}$标记的列仅在$\delta_1\delta_2\cdots\delta_r$行处为1，而在其它各行处均为0。

例如表1-3中，最小集$M_{110}=A\cap B\cap C'$，当且仅当$u\in A$，$u\in B$，$u\in C'$时，即当且仅当$u\in A$，$u\in B$，$u\notin C$时，$u\in M_{110}$，即M_{110}所标记的列仅在行110处取1，而在其它各行处为0。

表1-3

A	B	C	$A'\cap B'\cap C$ $=M_{001}$	$A'\cap B\cap C$ $=M_{011}$	$A\cap B\cap C'$ $=M_{110}$	$A\cap B\cap C$ $=M_{111}$	$M_{001}\cup M_{011}\cup M_{110}\cup M_{111}$
0	0	0	0	0	0	0	0
0	0	1	1	0	0	0	1
0	1	0	0	[illegible]	0	0	0
0	1	1	0	1	0	0	1
1	0	0	0	0	0	0	0
1	0	1	0	0	0	0	0
1	1	0	0	0	1	0	1
1	1	1	0	0	0	1	1

再考察由 $A_1,A_2,\cdots,A_r$ 产生的任意 i 个($i\leqslant 2^r$)不同最小集的并集 $M_{\delta_{11}\delta_{12}\cdots\delta_{1r}}\cup M_{\delta_{21}\delta_{22}\cdots\delta_{2r}}\cup\cdots\cup M_{\delta_{i1}\delta_{i2}\cdots\delta_{ir}}$ 和它的成员表。作出其列为 $A_1,A_2,\cdots,A_r$, $M_{\delta_{11}\delta_{12}\cdots\delta_{1r}}$, $M_{\delta_{21}\delta_{22}\cdots\delta_{2r}}$, $\cdots$, $M_{\delta_{i1}\delta_{i2}\cdots\delta_{ir}}$ 以及 $M_{\delta_{11}\delta_{12}\cdots\delta_{1r}}\cup M_{\delta_{21}\delta_{22}\cdots\delta_{2r}}\cup\cdots\cup M_{\delta_{i1}\delta_{i2}\cdots\delta_{ir}}$ 所标记的成员表，其最后一列可由它前面的 i 列借助 $\cup$ 运算的定义表1-1(b)而直接得到。显然，上述并集所标记的列仅在 $\delta_{11}\delta_{12}\cdots\delta_{1r}$, $\delta_{21}\delta_{22}\cdots\delta_{2r}$, $\cdots$, $\delta_{i1}\delta_{i2}\cdots\delta_{ir}$ 这 i 行处为1，在其它各行处为0。例如，表1-3说明了集合 $(A'\cap B'\cap C)\cup(A'\cap B\cap C)\cup(A\cap B\cap C')\cup(A\cap B\cap C)$ 的成员表的构造方法。

由最小集和最小集的并集的成员表的上述特点，我们有下面的定理。

定理1-4 由 $A_1,A_2,\cdots,A_r$ 产生的每个非空集合 S 恒可表示为由 $A_1,A_2,\cdots,A_r$ 产生的不同最小集的并集。

证明 由假设 $S\neq\phi$，因此在 S 的成员表里 S 所标记的列中必有 l 个1($1\leqslant l\leqslant 2^r$)。设这 l 个1分别在 $\delta_{11}\delta_{12}\cdots\delta_{1r}$, $\delta_{21}\delta_{22}\cdots\delta_{2r}$, $\cdots$, $\delta_{l1}\delta_{l2}\cdots\delta_{lr}$ 行处。作如下最小集的并集，并用 T 表示，即

$$T=M_{\delta_{11}\delta_{12}\cdots\delta_{1r}}\cup M_{\delta_{21}\delta_{22}\cdots\delta_{2r}}\cup\cdots\cup M_{\delta_{l1}\delta_{l2}\cdots\delta_{lr}}.$$

将 T 所标记的列加到 S 的成员表中，由前述的讨论，它必与 S 所标记的列恒同，因此 $S=T$。证完。

当一个集合被表示为不同最小集的并的形式时，我们称它为该集合的**最小集标准形式**。每一个非空集合必能表示为这种形式。

定理 1-4 的证明不仅肯定了集合的最小集标准形式，而且给出了构造集合的最小集标准形式的如下方法。

算法 1-1：

找出由 $A_1, A_2, \cdots, A_r$ 产生的集合 S 的最小集标准形式：

（1）构造 S 的成员表。若 S 标记的列不包含 1，则 $S=\phi$。否则

（2）若 S 列在 $\delta_{11}\delta_{12}\cdots\delta_{1r}$，$\delta_{21}\delta_{22}\cdots\delta_{2r}$，$\cdots$，$\delta_{l1}\delta_{l2}\cdots\delta_{lr}$ 行处为 1，则 S 的最小集标准形式由

$$S=\bigcup_{i=1}^{l}\left(\bigcap_{j=1}^{r}A_{ij}\right)$$

给出，其中

$$A_{ij}=\begin{cases}A_j' & \text{当 } \delta_{ij}=0;\\ A_j & \text{当 } \delta_{ij}=1.\end{cases}$$

例如，从表 1-2 看出集合 $(A\cap B)\cup(A'\cap C)$ 所标记的列在 001, 011, 110, 111 这些行处为 1，因此 $(A\cap B)\cup(A'\cap C)$ 的最小集标准形式为：

$$(A'\cap B'\cap C)\cup(A'\cap B\cap C)\cup(A\cap B\cap C')\cup(A\cap B\cap C).$$

（二） 最大集标准形式

定义1-14 设 $A_1, A_2, \cdots, A_r$ 是全集合 U 的子集，形为 $\bigcup_{i=1}^{r}\overline{A}_i$ 的集合称为由 $A_1, A_2, \cdots, A_r$ 所产生的**最大集**，其中每一个 $\overline{A}_i$ 为 A_i 或 A_i'。

显然，由 $A_1, A_2, \cdots, A_r$ 所产生的最大集共有 2^r 个。与最小集

不同，由 $A_1, A_2, \cdots, A_r$ 所产生的最大集的集合不构成U的分划．这一情况是明显的。

为了方便，我们用 $\overline{M}_{\delta_1\delta_2\cdots\delta_r}$ 表示最大集 $\overline{A}_1 \cup \overline{A}_2 \cup \cdots \cup \overline{A}_r$，其中

$$\delta_i = \begin{cases} 0 & \text{当 } \overline{A}_i = A_i; \\ 1 & \text{当 } \overline{A}_i = A'_i. \end{cases}$$

例如，$A_1 \cup A_2 \cup A'_3 \cup A_4$ 表示为 $\overline{M}_{0010}$，$A'_1 \cup A'_2 \cup A_3 \cup A_4$ 表示为 $\overline{M}_{1100}$。这样 $\overline{M}_{\delta_1\delta_2\cdots\delta_r}$ 的下标便唯一地描述了所要表示的最大集。

考察最大集 $\overline{M}_{\delta_1\delta_2\cdots\delta_r}$ 和它的成员表，作类似于最小集的讨论可知，$\overline{M}_{\delta_1\delta_2\cdots\delta_r}$ 所标记的列仅在 $\delta_1\delta_2\cdots\delta_r$ 行处为0，而在其它各行处均为 1。

例如在表1-4中，最大集$\overline{M}_{010} = A \cup B' \cup C$，当且仅当 $u \notin A$，$u \notin B'$，$u \notin C$ 时，即当且仅当 $u \notin A$，$u \in B$，$u \notin C$ 时，$u \notin \overline{M}_{010}$，即 $\overline{M}_{010}$ 所标记的列仅在行 010 处取 0，而在其它各行处均为 1。

表 1-4

A B C	$A \cup B \cup C = \overline{M}_{000}$	$A \cup B' \cup C = \overline{M}_{010}$	$A' \cup B \cup C = \overline{M}_{100}$	$A' \cup B \cup C' = \overline{M}_{101}$	$\overline{M}_{000} \cap \overline{M}_{010} \cap \overline{M}_{110} \cap \overline{M}_{101}$
0 0 0	[illegible]	1	1	1	0
0 0 1	1	1	1	1	1
0 1 0	1	[illegible]	1	1	0
0 1 1	1	1	1	1	1
1 0 0	1	1	0	1	0
1 0 1	1	1	1	0	0
1 1 0	1	1	1	1	1
1 1 1	1	1	1	1	1

再考察由 $A_1, A_2, \cdots, A_r$ 产生的任意 i 个（$i \leqslant 2^r$）不同最大集的交集 $\overline{M}_{\delta_{11}\delta_{12}\cdots\delta_{1r}} \cap \overline{M}_{\delta_{21}\delta_{22}\cdots\delta_{2r}} \cap \cdots \cap \overline{M}_{\delta_{i1}\delta_{i2}\cdots\delta_{ir}}$ 和它的成员表，作类似于最小集的讨论可知，上述交集所标记的列仅在 $\delta_{11}\delta_{12}\cdots\delta_{1r}$，$\delta_{21}\delta_{22}\cdots\delta_{2r}$，…，$\delta_{i1}\delta_{i2}\cdots\delta_{ir}$ 这 i 行处为 0，而在其它各行处为 1。例如，表1-4说明了集合 $(A \cup B \cup C) \cap (A \cup B' \cup C) \cap (A' \cup B \cup C) \cap (A' \cup B \cup C')$ 的成员表的构造方法。

类似于定理 1-4，我们有：

定理 1-5 由 $A_1, A_2, \cdots, A_r$ 产生的任一集合或为全集合 U 或为由 $A_1, A_2, \cdots, A_r$ 所产生的不同最大集的交集。

本定理的证明方法与定理 1-4 完全类似。

当一个集合被表示为不同最大集的交的形式时，我们称它为该集合的**最大集标准形式**。定理 1-5 的证明给出了构造这一形式的方法。

算法 1-2：

找出由 $A_1, A_2, \cdots, A_r$ 产生的集合 S 的最大集标准形式：

（1） 构造 S 的成员表，若 S 标记的列不包含 0，则 $S = U$。否则

（2） 若 S 列在 $\delta_{11}\delta_{12}\cdots\delta_{1r}$，$\delta_{21}\delta_{22}\cdots\delta_{2r}$，…，$\delta_{l1}\delta_{l2}\cdots\delta_{lr}$ 行处为 0，则 S 的最大集标准形式，由

$$S = \bigcap_{i=1}^{l}\left(\bigcup_{j=1}^{r} A_{ij}\right)$$

给出，其中

$$A_{ij} = \begin{cases} A_j & \text{当 } \delta_{ij} = 0; \\ A_j' & \text{当 } \delta_{ij} = 1. \end{cases}$$

例如，从表 1-2 看出集合 $(A \cap B) \cup (A' \cap C)$ 所标记的列在行 000，010，100 和 101 处为 0。因此 $(A \cap B) \cup (A' \cap C)$ 的最大集标准形式为：

$(A \cup B \cup C) \cap (A \cup B' \cup C) \cap (A' \cup B \cup C) \cap (A' \cup B \cup C')$。

（三） 集合标准形式的进一步说明

如果我们把空集 ϕ 看作是空集自身的最小集标准形式，把全集 U 看作是全集自身的最大集标准形式，那么，就可得出这样的结论：每一个集合都能表示为最小集标准形式和最大集标准形式。而且根据算法 1-1 和算法 1-2 可构造出这两个标准形式。

例如，设集合 $S=B\cap(A\cup(B\cap C'))$，为找出 S 的最小集和最大集标准形式，我们首先构造 S 的成员表：

A	B	C	C'	$B\cap C'$	$A\cup(B\cap C')$	$B\cap(A\cup(B\cap C'))$
0	0	0	1	0	0	0
0	0	1	0	0	0	0
0	1	0	1	1	1	1
0	1	1	0	0	0	0
1	0	0	1	0	1	0
1	0	1	0	0	1	0
1	1	0	1	1	1	1
1	1	1	0	0	1	1

因为 S 所标记的列在 010，110，111 行处为 1，所以 S 的最小集标准形式为：

$$S=M_{010}\cup M_{110}\cup M_{111}$$
$$=(A'\cap B\cap C')\cup(A\cap B\cap C')\cup(A\cap B\cap C).$$

S 所标记的列在 000，001，011，100，101 行处为 0，所以 S 的最大集标准形式为：

$$S=\overline{M}_{000}\cap\overline{M}_{001}\cap\overline{M}_{011}\cap\overline{M}_{100}\cap\overline{M}_{101}$$
$$=(A\cup B\cup C)\cap(A\cup B\cup C')\cap(A\cup B'\cup C')\cap$$
$$(A'\cup B\cup C)\cap(A'\cup B\cup C').$$

一般地，若集合 S 由算法 1-1 和算法 1-2 构造出的最小集和最大集标准形式分别为：

$$S = M_{\delta_{11}\delta_{12}\cdots\delta_{1r}} \cup M_{\delta_{21}\delta_{22}\cdots\delta_{2r}} \cup \cdots \cup M_{\delta_{l1}\delta_{l2}\cdots\delta_{lr}}$$

$$S = \overline{M}_{\bar{\delta}_{11}\bar{\delta}_{12}\cdots\bar{\delta}_{1r}} \cap \overline{M}_{\bar{\delta}_{21}\bar{\delta}_{22}\cdots\bar{\delta}_{2r}} \cap \cdots \cap \overline{M}_{\bar{\delta}_{m1}\bar{\delta}_{m2}\cdots\bar{\delta}_{mr}}$$

则行集合

$$\{\delta_{11}\delta_{12}\cdots\delta_{1r}, \delta_{21}\delta_{22}\cdots\delta_{2r}, \cdots, \delta_{l1}\delta_{l2}\cdots\delta_{lr}\}$$

与

$$\{\bar{\delta}_{11}\bar{\delta}_{12}\cdots\bar{\delta}_{1r}, \bar{\delta}_{21}\bar{\delta}_{22}\cdots\bar{\delta}_{2r}, \cdots, \bar{\delta}_{m1}\bar{\delta}_{m2}\cdots\bar{\delta}_{mr}\}$$

是不相交的，它们的并等于 S 成员表中所有 2^r 个行的集合. 因此，如果 S 的最小集标准形式是 l 个最小集的并，则最大集标准形式就是 2^r-l 个最大集的交。而且如果一种形式已知，则另一种形式也可直接构造出来。

下面我们介绍另一种求集合标准形式的算法，它不需要求助于成员表，使得标准形式的构造非常容易。

算法 1-3(1-4)：

求出由 $A_1, A_2, \cdots, A_r$ 产生的集合 S 的最小集（最大集）标准形式：

(1) 运用集合运算的定律，将 S 表示成 $\phi(U)$，或表示为形如 $\overline{A}_{i_1} \cap \overline{A}_{i_2} \cap \cdots \cap \overline{A}_{i_k}$($\overline{A}_{i_1} \cup \overline{A}_{i_2} \cup \cdots \cup \overline{A}_{i_k}$) 的不同交集（并集）的并（交），其中 $i_1 < i_2 < \cdots < i_k$。若 $S = \phi(S = U)$，则 S 就是所希望的形式。否则

(2) 如果每个交集（并集）为最小集（最大集），则 S 为所希望的形式。否则

(3) 从所得的表达式中，选取形如 $\overline{A}_{i_1} \cap \overline{A}_{i_2} \cap \cdots \cap \overline{A}_{i_k}$($\overline{A}_{i_1} \cup \overline{A}_{i_2} \cup \cdots \cup \overline{A}_{i_k}$)的一个交集(并集)，其中 $k < r$，对不出现于其中的某个 $\overline{A}_{i_h}$，用 $(\overline{A}_{i_1} \cap \overline{A}_{i_2} \cap \cdots \cap \overline{A}_{i_k} \cap \overline{A}_{i_h}) \cup (\overline{A}_{i_1} \cap \overline{A}_{i_2} \cap \cdots \cap \overline{A}_{i_k} \cap \overline{A}'_{i_h})$（用 $(\overline{A}_{i_1} \cup \overline{A}_{i_2} \cup \cdots \cup \overline{A}_{i_k} \cup \overline{A}_{i_h}) \cap (\overline{A}_{i_1} \cup \overline{A}_{i_2} \cup \cdots \cup \overline{A}_{i_k} \cup \overline{A}'_{i_h})$）代替这个交集(并集)，在新的交集(并集)中，按下标的升高次序重新排列 $\overline{A}_i$，删去完全相同的交集(并集)。返回到步骤 (2)。

例如，运用算法 1-3 构造 $S = B \cap (A \cup (B \cap C'))$ 的最小集标准形式：

$$\begin{aligned}
S &= B\cap(A\cup(B\cap C')) \\
&= (B\cap A)\cup(B\cap B\cap C') \\
&= (A\cap B\cap C)\cup(A\cap B\cap C')\cup(B\cap C') \\
&= (A\cap B\cap C)\cup(A\cap B\cap C')\cup(A\cap B\cap C') \\
&\qquad\qquad \cup(A'\cap B\cap C') \\
&= (A\cap B\cap C)\cup(A\cap B\cap C')\cup(A'\cap B\cap C').
\end{aligned}$$

运用算法 1-4 构造 S 的最大集标准形式：

$$\begin{aligned}
S &= B\cap(A\cup(B\cap C')) \\
&= B\cap(A\cup B)\cap(A\cup C') \\
&= (A\cup B)\cap(A'\cup B)\cap(A\cup C') \\
&= (A\cup B\cup C)\cap(A\cup B\cup C')\cap(A'\cup B\cup C)\cap \\
&\qquad (A'\cup B\cup C')\cap(A\cup B\cup C')\cap(A\cup B'\cup C') \\
&= (A\cup B\cup C)\cap(A\cup B\cup C')\cap(A'\cup B\cup C)\cap \\
&\qquad (A'\cup B\cup C')\cap(A\cup B'\cup C').
\end{aligned}$$

通过上述例子我们发现，无论用算法1-1(算法1-2)还是用算法1-3(算法1-4)，所得到的同一集合 S 的最小集(最大集)标准形式，除了最小集(最大集)的排列次序可能不同外，是相同的。其原因在于任一集合 S 的标准形式是唯一的。

定理 1-6　设 S 是由 $A_1, A_2, \cdots, A_r$ 所产生的集合，若不计最小集(最大集)的排列次序，则 S 的最小集(最大集)标准形式是唯一的。

定理 1-7 是定理 1-6 的直接推论。

定理 1-7　由 $A_1, A_2, \cdots, A_r$ 产生的两个集合，当且仅当它们的最小集(最大集)标准形式相同时，这两个集合相等。

上述定理的证明都很简单，请读者自己给出。

集合的上述两种标准形式，使得由 $A_1, A_2, \cdots, A_r$ 产生的集合往往能被化简，而且借助于这两种形式，我们能判断任意两个这样的集合是否相等。

§1.10 多重集合

前面说过，一个集合是一些不同对象的聚集。可是在许多场合会遇到聚集中有相同的对象。例如，考虑一个学校中所有学生的名册，其中可能有两个或者更多个学生有相同的名字；200个大小相同并涂上了颜色的彩球，其中有一些彩球的颜色可能也是相同的，等等。因此我们有必要引进多重集合的概念。所谓**多重集合**是不必一定要由不同的对象组成的聚集。例如，$\{a,b,b,c,c,c\}$、$\{a,a,a,a\}$和$\{a,b,c\}$都是多重集合。多重集合中，一个元素的**重复度**定义为该元素在多重集合里出现的次数，因此多重集合$\{a,b,b,c,c,c,\}$里的元素a的重复度是1，元素b的重复度是2，元素c的重复度是3，而元素d的重复度可看作是0。由此可见，原来定义的集合是多重集合里元素重复度为0或1的特殊情形。一个多重集合的基数定义为由它对应的假定所有元素都不相同的集合的基数。

设A和B是两个多重集合，A和B的并集记为$A\cup B$，它是多重集合，其中每个元素的重复度等于该元素在A和B中的重复度的最大值。例如，对于$A=\{a,b,b,c,c,c\}$和$B=\{a,a,b,c,d\}$，

$$A\cup B=\{a,a,b,b,c,c,c,d\}.$$

A和B的交集记为$A\cap B$，它是一个多重集合，其中每个元素的重复度等于该元素在A和B中的重复度的最小值。例如上述两个集合的交

$$A\cap B=\{a,b,c\}.$$

设多重集合$A=\{$电机工程师，电机工程师，电机工程师，机械工程师，数学家，制图员$\}$是某工程设计的第一阶段所需要的全体工作人员。多重集合$B=\{$电机工程师，机械工程师，机械工程师，数学家，计算机科学家，计算机科学家$\}$是该工程设计的

第二阶段所需要的全体工作人员，则多重集合 $A\cup B$ 是这个工程设计应该聘请的全体工作人员。多重集合 $A\cap B$ 是在工程设计的两个阶段都必须参加的全体工作人员。

多重集合 A 与 B 的差集记作 $A-B$，它是一个多重集合，当某一元素在 A 中的重复度减去在 B 中的重复度的差为正数时，就令此正数为该元素在 $A-B$ 中的重复度，否则该元素在 $A-B$ 中的重复度为零。例如设 $A=\{a,a,a,b,b,c,d,d,e\}$ 和 $B=\{a,a,b,b,b,c,c,d,d\}$，则

$$A-B=\{a,e\}.$$

在关于工程设计的工作人员的例中，多重集合 $A-B$ 是指在工程设计的第一阶段之后，需要重新分配工作的人员。

注意，多重集合的并、交、差的定义同集合中的有关定义完全一致。

最后，我们定义两个多重集合 A 与 B 的和集记为 $A+B$，它是一个多重集合，其中每一个元素的重复度等于该元素在 A 和 B 中的重复度之和。例如设 $A=\{a,a,b,c,c\}$ 和 $B=\{a,b,b,d\}$，则

$$A+B=\{a,a,a,b,b,b,c,c,d\}.$$

设 A 是某一天到校图书馆查阅资料的所有学生的多重集合，B 是第二天去查阅资料的所有学生的多重集合。这里 A 和 B 之所以是多重集合，是因为在一天里，一个学生可能要多次去图书馆查阅资料。因此，$A+B$ 就是这两天到图书馆查阅资料的学生数的一个总记录。

今后，如果我们不作特别声明，所谓"集合"概指 §1.1 中所定义的集合。

习　　题

1. 列举下列集合的元素：

(1) 小于20的素数的集合；

(2) 小于 5 的非负整数的集合；

(3) $\{i \mid i \in I,\ i^2 - 10i - 24 < 0$ 且 $5 \leqslant i \leqslant 15\}$。

2. 用描述法表示下列集合：

(1) $\{a_1, a_2, a_3, a_4, a_5\}$；

(2) $\{2, 4, 8, \cdots\}$；

(3) $\{0, 2, 4, 6, 8, \cdots, 98, 100\}$。

3. 设已知下列各集合：

$A = \{x \mid x \in I,\ x < 10\}$，$B = \{x \mid x \in I,\ x > 3\}$，

$C = \{x \mid x$ 是一个英文字母$\}$，$D = \{a, b, c, d, e, 1, 2, 3, 4, 5\}$，

在空白中填上一个适当的元素。

____ $\in A$，____ $\in D$，____ $\in A$ 但 $\notin D$，____ $\in C$ 同时 $\in D$，____ $\in A$ 同时 $\in B$，____ $\in B$ 但 $\notin A$，____ $\in B$ 但 $\notin C$，____ $\in A$，$\in B$ 但 $\notin D$。

4. 下面哪些式子是错误的？

(1) $\{a\} \in \{\{a\}\}$；

(2) $\{a\} \subseteq \{\{a\}\}$；

(3) $\{a\} \in \{\{a\}, a\}$；

(4) $\{a\} \subseteq \{\{a\}, a\}$。

5. 已给 $S = \{2, a, \{3\}, 4\}$ 和 $R = \{\{a\}, 3, 4, 1\}$，指出下面哪些论断是正确的？哪些是错误的？

(1) $\{a\} \in S$；

(2) $\{a\} \in R$；

(3) $\{a, 4, \{3\}\} \subseteq S$；

(4) $\{\{a\}, 1, 3, 4\} \subseteq R$；

(5) $R = S$；

(6) $\{a\} \subseteq S$；

(7) $\{a\} \subseteq R$；

(8) $\phi \subset R$；

(9) $\phi \subseteq \{\{a\}\} \subseteq R$；

(10) $\{\phi\} \subseteq S$；

(11) $\phi \in R$；

(12) $\phi \subseteq \{\{3\}, 4\}$。

6. 举出集合 A、B、C 的例子，使其满足 $A\in B$，$B\in C$ 且 $A\notin C$.

7. 给出下列集合的幂集：

(1) $\{a,\{b\}\}$；　　(2) $\{\phi,a,\{a\}\}$.

8. 设 $A=\{a\}$，给出 A 和 2^A 的幂集.

9. 设 $A=\{a_1,a_2,\cdots,a_8\}$，由 B_{17} 和 B_{31} 所表示的 A 的子集各是什么？应如何表示子集 $\{a_2,a_6,a_7\}$ 和 $\{a_1,a_8\}$？

10. 设 $U=\{1,2,3,4,5\}$，$A=\{1,4\}$，$B=\{1,2,5\}$，$C=\{2,4\}$，确定集合：

(1) $A\cap B'$；　　(6) $A'\cup B'$；

(2) $(A\cap B)\cup C'$；　　(7) $(B\cup C)'$；

(3) $A\cup(B\cap C)$；　　(8) $B'\cap C'$；

(4) $(A\cup B)\cap(A\cup C)$；　　(9) 2^A-2^C；

(5) $(A\cap B)'$；　　(10) $2^A\cap 2^C$.

11. 给定自然数集 N 的下列子集：

$A=\{1,2,7,8\}$；

$B=\{i\mid i^2<50\}$；

$C=\{i\mid i$ 可被 3 整除，$0\leqslant i\leqslant 30\}$；

$D=\{i\mid i=2^k,\ k\in Z,\ 0\leqslant k\leqslant 6\}$，

求下列集合：

(1) $A\cup(B\cup(C\cup D))$；　　(3) $B-(A\cup C)$；

(2) $A\cap(B\cap(C\cap D))$；　　(4) $(A'\cap B)\cup D$.

12. 给定自然数集 N 的下列子集：

$A=\{n\mid n<12\}$；　　$D=\{n\mid n=3k,\ k\in N\}$；

$B=\{n\mid n\leqslant 8\}$；　　$E=\{n\mid n=2k-1,\ k\in N\}$，

$C=\{n\mid n=2k,\ k\in N\}$；

将下列集合表示为由 A、B、C、D、E 产生的集合：

(1) $\{2,4,6,8\}$；　　(3) $\{10\}$；

(2) $\{3,6,9\}$；　　(4) $\{n\mid n=3$ 或 $n=6$ 或 $n\geqslant 9\}$；

(5) $\{n|n$ 是偶数且 $n\leqslant 10$ 或 n 是奇数且 $n>9\}$；

(6) $\{n|n$ 是 6 的倍数$\}$。

13. 判断以下哪些论断是正确的，哪些论断是错误的。并说明理由。

(1) 若 $a\in A$，则 $a\in A\cup B$；

(2) 若 $a\in A$，则 $a\in A\cap B$；

(3) 若 $a\in A\cap B$，则 $a\in B$；

(4) 若 $A\subseteq B$，则 $A\cap B=B$；

(5) 若 $A\subseteq B$，则 $A\cap B=A$；

(6) 若 $a\notin A$，则 $a\in A\cup B$；

(7) 若 $a\notin A$，则 $a\in A\cap B$。

14. 设 A、B、C 是任意的集合，下述论断哪些是正确的？

(1) 若 $A\cap B=A\cap C$，则 $B=C$；

(2) 当且仅当 $A\cup B=B$，有 $A\subseteq B$；

(3) 当且仅当 $A\cap B=A$，有 $A\subseteq B$；

(4) 当且仅当 $A\subseteq C$，有 $A\cap(B-C)=\phi$；

(5) 当且仅当 $B\subseteq C$，有 $(A-B)\cup C=A$。

15. 设 A、B、C 和 D 是集合，下述论断哪些是正确的？

(1) 若 $A\subseteq B$，$C\subseteq D$，则 $(A\cup C)\subseteq(B\cup D)$；

(2) 若 $A\subseteq B$，$C\subseteq D$，则 $(A\cap C)\subseteq(B\cap D)$；

(3) 若 $A\subset B$，$C\subset D$，则 $(A\cup C)\subset(B\cup D)$；

(4) 若 $A\subset B$，$C\subset D$，则 $(A\cap C)\subset(B\cap D)$。

16. 设 A、B 是两个集合，

(1) 如果 $A-B=B$，那么 A 和 B 有什么关系？

(2) 如果 $A-B=B-A$，那么 A 和 B 有什么关系？

17. 在一个班级的 50 个学生中，有 26 人在离散数学的考试中取得了优秀的成绩；有21人在程序设计的考试中取得了优秀的成绩。假如有17人两次考试中都没有取得优秀成绩，问有多少学生

在两次考试中都得到了优秀成绩？

18. 设A、B、C是任意集合，运用成员表证明：

(1) $(A\cup B)\cap(A'\cup C)=(A\cap C)\cup(A'\cap B)$；

(2) $(A\cup B)\cap(A\cup C)=A\cup(B\cap C)$；

(3) $A-(B\cup C)=(A-B)\cap(A-C)$；

(4) $A-(B\cap C)=(A-B)\cup(A-C)$。

19. 由S和T的成员表如何判断$S\subseteq T$？应用成员表证明或否定$(A\cup B)\cap(B\cup C)'\subseteq A\cap B'$。

20. $A_1,A_2,\cdots,A_n$为U的子集，$A_1,A_2,\cdots,A_n$至多能产生多少不同的子集？

21. 证明分配律、等幂律和吸收律9'。

22. 设A、B、C是任意集合，运用集合运算定律证明：

(1) $B\cup((A'\cup B)\cap A)'=U$；

(2) $(A\cup B)\cap(B\cup C)\cap(C\cup A)=(A\cap B)\cup(B\cap C)\cup(C\cap A)$；

(3) $(A\cup B)\cap(B\cup C)\cap(A\cup C)=(A\cap B)\cup(A'\cap B\cap C)\cup(A\cap B'\cap C)$。

23. 用德·摩根定律证明$(A\cap B')\cup(A'\cap(B\cup C'))$的补集是$(A'\cup B)\cap(A\cup B')\cap(A\cup C)$。

24. 设A为某些实数的集合，定义为

$$A_0=\{a\mid a<1\},$$

$$A_i=\left\{a\mid a\leqslant 1-\frac{1}{i}\right\}\quad(i=1,2,\cdots).$$

证明：$\bigcup_{i=1}^{\infty}A_i=A_0$。

25. 设$\{A_1,A_2,\cdots,A_r\}$是集合A的一个分划，证明：$A_1\cap B$、$A_2\cap B$、$\cdots$、$A_r\cap B$中所有非空集合构成$A\cap B$的一个分划。

26. n个元素的集合，有多少种不同的方法分划成为两块？

27. 找出由A、B产生的如下集合的最小集标准形式：

(1) U;　　　　(3) A';

(2) A;　　　　(4) $A\cup B$.

28. 找出由A、B产生的如下集合的最大集标准形式:

(1) ϕ;　　　　(3) A';

(2) A;　　　　(4) $A\cap B$.

29. 找出下列集合的最小集和最大集标准形式:

(1) $(A\cap B')\cup(B\cap(A\cup C'))$　(由A、B、C产生);

(2) $((A\cup D')\cap(B'\cup C)')\cup(A\cap B\cap D)$　(由A、B、C、D产生)。

30. S是一集合，其最小集标准形式由

$$S=M_{\delta_{11}\delta_{12}\cdots\delta_{1n}}\cup M_{\delta_{21}\delta_{22}\cdots\delta_{2n}}\cup\cdots\cup M_{\delta_{k1}\delta_{k2}\cdots\delta_{kn}}$$

给出，证明S'的最大集标准形式为

$$S'=\overline{M}_{\delta_{11}\delta_{12}\cdots\delta_{1n}}\cap M_{\delta_{21}\delta_{22}\cdots\delta_{2n}}\cap\cdots\cap M_{\delta_{k1}\delta_{k2}\cdots\delta_{kn}}$$

31. 运用最小集和最大集标准形式证明:

$(A\cap B')\cup(A'\cap(B\cup C'))$的补集是$(A'\cup B)\cap(A\cup B')\cap(A\cup C)$.

第二章 关　系

与集合的概念一样，关系的概念在计算机科学中也是最基本的。它在有限自动机和形式语言理论中，在应用领域如编译程序设计、信息检索和数据结构的描写中经常出现。在算法分析和程序结构中，关系的概念也起着重要的作用。

这一章介绍n元组和笛卡尔积以及由笛卡尔积引出的关系的概念；说明如何用矩阵和图来表示关系；定义关系的复合运算；列举关系的几个主要性质；介绍两类重要的关系，等价关系和偏序关系；说明由等价关系如何导出分划，并介绍由这样的分划所定义的商集的概念。最后讨论称为偏序（全序和良序作为特殊情形）的关系。

§2.1 笛卡尔积

由n个具有给定次序的个体组成的序列，称为**有序n元组**，记作$(a_1, a_2, \cdots, a_n)$的形式。

有序n元组$(a_1, a_2, \cdots, a_n)$中的第i个元素a_i，常称为该有序n元组的第i个坐标。

注意，一个有序n元组不是由n个元素组成的集合。前者明确规定了元素的排列次序，而元素的集合则没有这一要求。

例如　　$(a, b, c) \neq (b, a, c) \neq (c, b, a)$,

但　　$\{a, b, c\} = \{b, a, c\} = \{c, b, a\}$.

又如　　$(a, a, a) \neq (a, a) \neq (a)$.

两个有序n元组$(a_1, a_2, \cdots, a_n)$和$(b_1, b_2, \cdots, b_n)$相等定义

为：当且仅当 $a_1=b_1$，$a_2=b_2$，…，$a_n=b_n$ 时，$(a_1,a_2,\cdots,a_n)=(b_1,b_2,\cdots,b_n)$。因此 $(1,2)\neq(2,1)$，$(1,1)\neq(2,2)$。

有序 n 元组的一种常见的特殊情形是 $n=2$。有序二元组 (a,b) 又被称为序偶．序偶的一个熟悉的例子是平面上点的笛卡尔坐标表示。例如，序偶 $(1,3)$、$(2,4)$ 和 $(3,1)$ 均表示平面上不同的点。

定义 2-1 设 $A_1,A_2,\cdots,A_n$ 是任意的集合，所有有序 n 元组 $(a_1,a_2,\cdots a_n)$ 的集合，称为 $A_1,A_2,\cdots,A_n$ 的**笛卡尔积**，用 $A_1\times A_2\times\cdots\times A_n$ 表示，其中 $a_1\in A_1,a_2\in A_2,\cdots,a_n\in A_n$，即

$$A_1\times A_2\times\cdots\times A_n=\{(a_1,a_2,\cdots,a_n)|a_i\in A_i\quad i=1,2,\cdots,n\}.$$

例 1 设 $A_1=\{0,1\}$，$A_2=\{2,3\}$，$A_3=\{1,4\}$，

则 $$A_1\times A_2\times A_3=\{(0,2,1),(0,2,4),(0,3,1),(0,3,4),(1,2,1),(1,2,4),(1,3,1),(1,3,4)\}.$$

例 2 设 $A=\{\alpha,\beta\}$，$B=\{1,2,3\}$，

则 $$A\times B=\{(\alpha,1),(\alpha,2),(\alpha,3),(\beta,1),(\beta,2),(\beta,3)\};$$
$$B\times A=\{(1,\alpha),(2,\alpha),(3,\alpha),(1,\beta),(2,\beta),(3,\beta)\};$$
$$A\times A=\{(\alpha,\alpha),(\alpha,\beta),(\beta,\alpha),(\beta,\beta)\};$$
$$B\times B=\{(1,1),(1,2),(1,3),(2,1),(2,2),(2,3),(3,1),(3,2),(3,3)\}.$$

由上可知 $$A\times B\neq B\times A.$$

例 3 设 $A=\phi$，$B=\{1,2,3\}$，

则 $$A\times B=B\times A=\phi.$$

若所有的 A_i 都是有限集，则 $A_1\times A_2\times\cdots\times A_n$ 也是有限集，

且 $$\#(A_1\times A_2\times\cdots\times A_n)=(\#A_1)\times(\#A_2)\times\cdots\times(\#A_n).$$

当所有的 A_i 都相同且等于 A 时，$A_1\times A_2\times\cdots\times A_n$ 可用 A^n 表示。

例 4 设 $A_1=R$（实数集），$A_2=R$，

则 $$A_1\times A_2=R\times R=\{(x,y)|x,y\in R\},$$

即 $R\times R$ 是平面上所有点的集合，序偶 (x,y) 中第一个元素 x 是相应点在笛卡尔坐标系中的横坐标，第二个元素 y 是相应点的纵坐标。

§2.2 关　系

在许多涉及离散对象的问题中，其对象中间往往存在某一类关系。例如在一组计算机程序中，如果两个程序共用某些数据，我们就可以说这两个程序是相关的，否则为无关的。在某两个班的学生中，如果一个班的某学生和另一个班的某学生有相同的姓，我们就可以说这两个学生是相关的，否则为无关的。又如考察集合 $\{1,2,3,\cdots,15\}$，如果此集合中三个整数之和能被 5 整除，我们就可以说这三个数是相关的，如 2、3、5 是相关的，5、10、15 是相关的，而 1、2、4 是无关的。这一章我们将研究离散对象之间的这一类关系，为此我们首先给出关系的定义。

定义 2-2　笛卡尔积 $A_1\times A_2\times\cdots\times A_n$ 的任意一个子集称为 $A_1,A_2,\cdots,A_n$ 上的一个 **n 元关系**。

一个最重要的特殊情形是 $n=2$，在这种情况下，关系是 $A_1\times A_2$ 的一个子集（一个序偶集，其第一个坐标取自 A_1，第二个座标取自 A_2），并称为由 A_1 到 A_2 的一个**二元关系**。下面主要讨论二元关系，因此，今后若无特别声明，则术语"关系"概指二元关系。

例 1　设有集合 $A=\{0,1\}$，$B=\{1,2,3\}$，

则　$\rho_1=\{(0,1),(0,3),(1,2)\}$ 是由 A 到 B 的一个关系，

而　$\rho_2=\{(1,0),(1,1),(2,1)\}$ 是由 B 到 A 的一个关系。

因为 ϕ 是任何集合的子集，所以 ϕ 也定义一种关系，称为**空关系**。

若 ρ 是由 A 到 B 的一个关系，且 $(a,b)\in\rho$，则我们说，和

对 b 有关系 ρ"，记作 $a\rho b$。如果 $(a,b)\notin\rho$，则记作 $a\rho' b$。于是对例 1 有

$$0\rho_1 1,\ 0\rho_1 3,\ 1\rho_1 2,\ 但\ 0\rho_1' 2,\ 1\rho_1' 1,\ 1\rho_1' 3.$$

$$1\rho_2 0,\ 1\rho_2 1,\ 2\rho_2 1,\ 但\ 2\rho_2' 0,\ 3\rho_2' 0,\ 3\rho_2' 1.$$

定义 2-3 设 ρ 是由 A 到 B 的一个关系，则使得 $a\rho b(b\in B)$ 成立的所有元素 $a\in A$ 的集合，称为关系 ρ 的**定义域**，记作 D_ρ；使得 $a\rho b(a\in A)$ 成立的所有元素 $b\in B$ 的集合，称为关系 ρ 的**值域**，记作 R_ρ，即

$$D_\rho=\{a\,|\,a\in A,\ 存在\ b\in B,\ 使得\ a\rho b\};$$

$$R_\rho=\{b\,|\,b\in B,\ 存在\ a\in A,\ 使得\ a\rho b\}.$$

由定义显然有 $D_\rho\subseteq A$，$R_\rho\subseteq B$。

例 2 考虑集合 $A=\{2,3,4\}$，$B=\{2,3,4,5,6\}$ 以及如下定义的由 A 到 B 的关系 ρ，当且仅当 a 能整除 b 时，$a\rho b$ 成立，于是

$$\rho=\{(2,2),(2,4),(2,6),(3,3),(3,6),(4,4)\}.$$

ρ 的定义域 $D_\rho=\{2,3,4\}$，ρ 的值域 $R_\rho=\{2,3,4,6\}$。

定义 2-4 设 A 和 B 是两个集合，ρ 是由 A 到 B 的关系，则由 B 到 A 的关系

$$\tilde{\rho}\triangleq\{(b,a)\,|\,(a,b)\in\rho\}$$

称为关系 ρ 的**逆关系**。

由定义 2-4 可知，只要将 ρ 的每一个序偶中元素次序加以颠倒，就可以得到逆关系 $\tilde{\rho}$ 的所有序偶。例如，例 2 中关系 ρ 的逆关系

$$\tilde{\rho}=\{(2,2),(4,2),(6,2),(3,3),(6,3),(4,4)\},$$

它是一个由 $B=\{2,3,4,5,6\}$ 到 $A=\{2,3,4\}$ 的关系。

图 2-1 给出了一个由 A 到 B 的关系的图示。在该图中，小圆标定的 a_i 和 b_j 分别表示 A 和 B 中的元素。当且仅当 $a_i\rho b_j$ 时，才有箭头从 a_i 指向 b_j。（将各箭头反向，就得到关系 $\tilde{\rho}$ 的图示）。

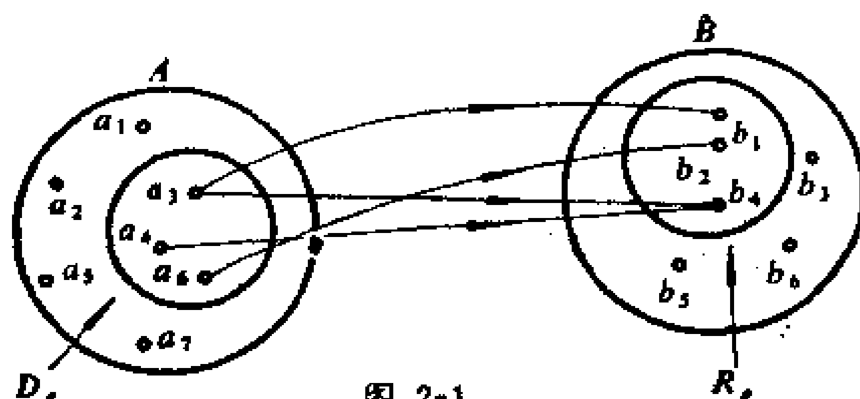


图 2-1

当A和B是有限集时，由A到B的关系ρ可以方便地用一个$(\#A)\times(\#B)$矩阵来表示，该矩阵称为ρ的**关系矩阵**，记作M_ρ

设集合 $A=\{a_1,a_2,\cdots,a_{\#A}\}$，$B=\{b_1,b_2,\cdots,b_{\#B}\}$，$\rho$是由$A$到$B$的关系，则关系矩阵$M_\rho$的第$i$行、$j$列的元素$r_{ij}$如下定义：

$$r_{ij}=\begin{cases}1 & 若\ a_i\rho b_j,\\ 0 & 若\ a_i\rho' b_j,\end{cases}$$

因此关系矩阵中的元素仅为1和0。

例如，例2中的关系ρ可用关系矩阵

$$M_\rho=\begin{matrix} & \begin{matrix}2 & 3 & 4 & 5 & 6\end{matrix} \\ \begin{matrix}2\\3\\4\end{matrix} & \begin{pmatrix}1 & 0 & 1 & 0 & 1\\ 0 & 1 & 0 & 0 & 1\\ 0 & 0 & 1 & 0 & 0\end{pmatrix}\end{matrix}$$

来表示。

关系矩阵为在计算机上表达关系提供了一种方法。将关系ρ的关系矩阵M_ρ的行和列加以交换，就得到关系$\tilde{\rho}$的关系矩阵，即$M_{\tilde{\rho}}=M_\rho$的转置。

二元关系的一种特殊情形，即由集合A到A自身的关系（是A^2的一个子集），称为**集合A上的关系**。

例3 设 $A=\{0,1,2,3\}$，则

$$\rho=\{(0,0),(0,3),(2,0),(2,1),(2,3),(3,2)\}$$

是集合 A 上的一个关系。

例 4 设有实数集 R，

而
$$\rho_1=\{(x,y)\mid(x,y)\in R^2,\ x<y\},$$
则 ρ_1 是实数集 R 上的一个关系，即常说的“小于”关系。例如序偶 $(3.5,5)\in\rho_1$，$(-1.2,0)\in\rho_1$ 而 $(5,1.005)\notin\rho_1$。类似地，实数集 R 上还可定义“等于”和“大于”关系，即
$$\rho_2=\{(x,y)\mid(x,y)\in R^2,\ x=y\};$$
$$\rho_3=\{(x,y)\mid(x,y)\in R^2,\ x>y\}.$$

这些关系的定义域是什么？值域是什么？它们在笛卡尔坐标平面上分别表示哪些点的集合？请读者自己作出回答。

若 $\rho=A^2$，则 ρ 叫做 A 上的**普遍关系**，用 U_A 表示，即
$$U_A=\{(a_i,a_j)\mid a_i,a_j\in A\}.$$

A 上的**恒等关系**用 I_A 表示，定义为
$$I_A=\{(a_i,a_i)\mid a_i\in A\}.$$

例 5 设 $A=\{0,1,2\}$，

则
$$U_A=\{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2),(2,0),(2,1),(2,2)\};$$
$$I_A=\{(0,0),(1,1),(2,2)\}.$$

一个有限集合 A 上的关系 ρ 不仅可以用上述的 $(\#A)\times(\#A)$ 矩阵来表示，也可以用一个称之为 ρ 的**关系图**的图形来表示。该图具有与 A 中元素个数相同的结点，每一个结点代表 A 中的一个元素，并画作一个带有元素标号的小圆圈。当且仅当有 $a_i\rho a_j$ 时，我们就用一条弧（或直线）连接结点

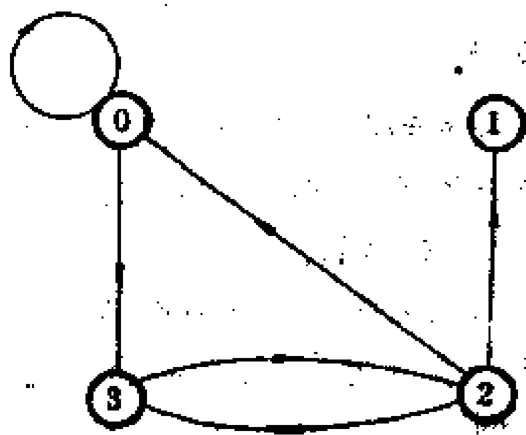


图2.2

a_i 和 a_j，并在弧上（或直线上）沿着从 a_i 到 a_j 的方向画一箭头．当对应于 ρ 中的序偶的所有结点都用带有适当箭头的弧（或直线）连接起来时，我们就得到了 ρ 的关系图（若将所有的箭头反向，就得到 $\tilde{\rho}$ 的关系图）．图 2-2 给出了例 3 中关系 ρ 的图．

图中每一条带有箭头的弧（或直线）称为该图的边．

对于图中任意两结点 a_i 到 a_j，若存在 $l-1$ 个结点 a_{k_1}，a_{k_2}，…，$a_{k_{l-1}}$，使得有 $a_i\rho a_{k_1}$，$a_{k_1}\rho a_{k_2}$，…，$a_{k_{l-1}}\rho a_j$，则我们就说从结点 a_i 到 a_j 有一条长为 l 的路（$l\geqslant1$）．若 $a_i=a_j$，这条路就成为一条回路．

例如，图 2-2 中对于结点 0 和 1，因为 $0\rho3$，$3\rho2$，$2\rho1$，所以从结点 0 到 1 有长为 3 的路．因为 $3\rho2$，$2\rho3$，所以从 3 到 3 有长为 2 的路．因为 $0\rho3$，所以从 0 到 3 有长为 1 的路．

§2.3 关系的复合

由于关系是一个集合，因此可对关系进行集合的运算，诸如求并、交、补等，从而产生其它新的关系．这些与一般集合一样地进行，这里不再详细讨论．本节将着重讨论对关系的另一种运算，即关系的复合运算．

定义 2-5 设 ρ_1 是一个由 A_1 到 A_2 的关系，ρ_2 是一个由 A_2 到 A_3 的关系，则 ρ_1 和 ρ_2 的**复合关系**是一个由 A_1 到 A_3 的关系用 $\rho_1\cdot\rho_2$ 表示（或简记作 $\rho_1\rho_2$），定义为当且仅当存在某个 $a_k\in A_2$ 使得 $a_i\rho_1a_k$，$a_k\rho_2a_j$ 时，有 $a_i(\rho_1\cdot\rho_2)a_j$．

这种从 ρ_1 和 ρ_2 得到 $\rho_1\cdot\rho_2$ 的运算，叫做**关系的复合运算**．

例 1 设 ρ_1 是一由 $A_1=\{1,2,3,4\}$ 到 $A_2=\{2,3,4\}$ 的关系，ρ_2 是一由 A_2 到 $A_3=\{1,2,3\}$ 的关系，它们分别为

$$\rho_1=\{(a_i,a_k)\,|\,a_i+a_k=5\}=\{(1,4),(2,3),(3,2)\};$$

$$\rho_2=\{(a_k,a_j)\,|\,a_k-a_j=2\}=\{(3,1),(4,2)\}.$$

复合关系 $\rho_1\cdot\rho_2$ 由所有这样的序偶 (a_i,a_j) 组成，存在某个 $a_k\in A_2$，使得 $a_i+a_k=5$ 且 $a_k-a_j=2$，于是

$$\rho_1\cdot\rho_2=\{(1,2),(2,1)\}.$$

图 2-3 给出了复合关系 $\rho_1\cdot\rho_2$ 的图示。

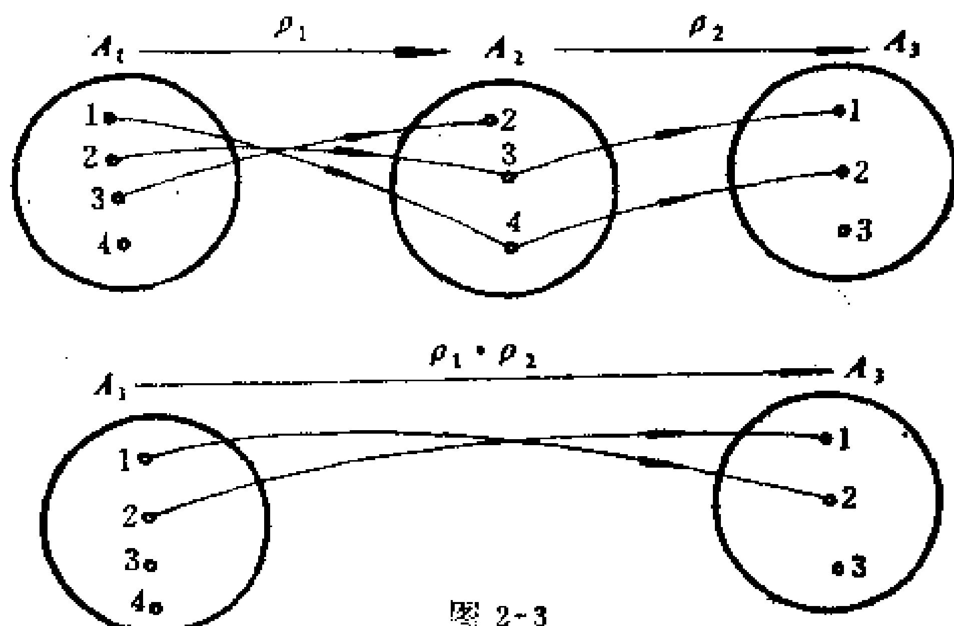


图 2-3

显然，如果 ρ_1 的值域和 ρ_2 的定义域的交集为空，则 $\rho_1\cdot\rho_2$ 是空关系。

设 ρ 是由集合 A 到集合 B 的关系，I_A 是集合 A 上的恒等关系，I_B 是集合 B 上的恒等关系，则由恒等关系的定义可知

$$I_A\cdot\rho=\rho\cdot I_B=\rho.$$

定理 2-1 设 ρ_1 是由 A_1 到 A_2 的关系，ρ_2 是由 A_2 到 A_3 的关系，ρ_3 是由 A_3 到 A_4 的关系，则有 $(\rho_1\cdot\rho_2)\cdot\rho_3=\rho_1\cdot(\rho_2\cdot\rho_3)$。

证明 根据复合关系的定义，$(\rho_1\cdot\rho_2)\cdot\rho_3$ 和 $\rho_1\cdot(\rho_2\cdot\rho_3)$ 同是由 A_1 到 A_4 的关系。

下面证明 $(\rho_1\cdot\rho_2)\cdot\rho_3\subseteq\rho_1\cdot(\rho_2\cdot\rho_3)$。

设 $(a,d)\in(\rho_1\cdot\rho_2)\cdot\rho_3$，由复合关系的定义，必有 $c\in A_3$ 使得 $a(\rho_1\cdot\rho_2)c$，$c\rho_3d$，又由 $a(\rho_1\cdot\rho_2)c$，必有 $b\in A_2$ 使得 $a\rho_1b$，$b\rho_2c$。

由 $b\rho_2 c$，$c\rho_3 d$，可得 $b(\rho_2\cdot\rho_3)d$，于是由 $a\rho_1 b$，$b(\rho_2\cdot\rho_3)d$，可得 $a(\rho_1\cdot(\rho_2\cdot\rho_3))d$，即 $(a,d)\in\rho_1\cdot(\rho_2\cdot\rho_3)$，故有 $(\rho_1\cdot\rho_2)\cdot\rho_3\subseteq\rho_1\cdot(\rho_2\cdot\rho_3)$。

类似地可以证明 $\rho_1\cdot(\rho_2\cdot\rho_3)\subseteq(\rho_1\cdot\rho_2)\cdot\rho_2$。

由此 $(\rho_1\cdot\rho_2)\cdot\rho_3=\rho_1\cdot(\rho_2\cdot\rho_3)$ 得证。

由于 $(\rho_1\cdot\rho_2)\cdot\rho_3$ 与 $\rho_1\cdot(\rho_2\cdot\rho_3)$ 相等，因此我们常删去括号将它们写作 $\rho_1\cdot\rho_2\cdot\rho_3$。一般地，若 ρ_1 是一由 A_1 到 A_2 的关系，ρ_2 是一由 A_2 到 A_3 的关系，…，ρ_n 是一由 A_n 到 A_{n+1} 的关系，则 $(\cdots((\rho_1\cdot\rho_2)\cdot\rho_3)\cdots\rho_{n-1})\rho_n$ 是一由 A_1 到 A_{n+1} 的关系。由归纳法容易证明，任意 n 个关系的复合也是可结合的。即在上式中只要不改变 n 个关系符号的次序，不论在它们中间怎样加括号，其结果是一样的，因此去括号的表达式 $\rho_1\rho_2\cdots\rho_n$ 唯一地表示一个由 A_1 到 A_{n+1} 的关系。

特别，当 $A_1=A_2=\cdots=A_n=A_{n+1}=A$ 且 $\rho_1=\rho_2=\cdots=\rho_n=\rho$ 时（即当所有的关系 ρ_i 都是集合 A 上同样的关系 ρ 时），复合关系 $\rho_1\rho_2\cdots\rho_n$ 可以用 ρ^n 表示（它是集合 A 上的一个关系）。

例 2 设 $A=\{1, 2, 3, 4\}$，A 上的关系 $\rho=\{(2,1),(3,2),(4,3)\}$，则有

$$\rho^2=\{(3,1),(4,2)\},$$
$$\rho^3=\{(4,1)\},$$
$$\rho^4=\phi.$$

§2.4 复合关系的关系矩阵和关系图

在讨论复合关系矩阵之前，我们先介绍布尔运算，并用布尔运算来定义两个关系矩阵的乘积。布尔运算只涉及数字 0 和 1，这些数字的加法和乘法按下列方式进行：

$$0+0=0,\quad 0+1=1+0=1+1=1,$$
$$1\cdot1=1,\quad 1\cdot0=0\cdot1=0\cdot0=0.$$

例如式子 $(1\cdot1)+(0\cdot0\cdot1)+(1\cdot1\cdot1)+1+(1\cdot0)=1$。

一般地，在一个式子中当且仅当至少有一个乘积是形式 $1\cdot1\cdots1$ 时，乘积的和等于 1，否则为 0。

下面用布尔运算来定义两个关系矩阵的乘积。

定义 2-6 设 M_1 是一个 (i,j) 通路（即第 i 行、j 列的元素）为 $r_{ij}^{(1)}$ 的 $l\times m$ 关系矩阵，M_2 是一个 (i,j) 通路为 $r_{ij}^{(2)}$ 的 $m\times n$ 关系矩阵，则 M_1 与 M_2 的乘积，记为 $M_1\cdot M_2$，是一个 $l\times n$ 关系矩阵，其 (i,j) 通路

$$r_{ij}=\sum_{k=1}^{m}(r_{ik}^{(1)}\cdot r_{kj}^{(2)})\quad (i=1,2,\cdots,l;\quad j=1,2,\cdots,n),$$

在这里全部加法和乘法都是布尔型的。

注意，M_1 的列数必须等于 M_2 的行数，这样 $M_1\cdot M_2$ 才有定义。

例 1 设 M_1 和 M_2 是两个关系矩阵，

$$M_1=\begin{pmatrix}0&0&0\\0&0&1\\0&1&0\\1&0&0\end{pmatrix},\qquad M_2=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix},$$

则

$$M_1\cdot M_2=\begin{pmatrix}0&0&0\\0&0&1\\0&1&0\\1&0&0\end{pmatrix}.$$

根据定义 2-6 容易证明，关系矩阵的乘积是可结合的，即乘积 $(M_1\cdot M_2)\cdot M_3$ 和 $M_1\cdot(M_2\cdot M_3)$ 当有定义时，是相等的。因此可以直接写成 $M_1\cdot M_2\cdot M_3$。一般地，若 $M_1\cdot M_2, M_2\cdot M_3, \cdots, M_{n-1}\cdot M_n$ 有定义，则去括号的式子 $M_1\cdot M_2\cdot\cdots\cdot M_n$ 唯一地表示 $M_1, M_2, \cdots, M_n$ 的乘积。特别，当这 n 个关系矩阵都相等时，

即 $M_1 = M_2 = \cdots = M_n = M$ 时，其乘积可用 M^n 表示。

假设 ρ_1 是由 A 到 B 的关系，ρ_2 是由 B 到 C 的关系，这里 A，B 和 C 都是有限集。由前节所述，复合关系 $\rho_1 \cdot \rho_2$ 是一由 A 到 C 的关系。本节的任务是探讨复合关系的关系矩阵与构成这一复合关系的各关系的关系矩阵之间的联系。下面先看一例。

例 2 设 ρ_1 是一由 $A=\{1,2,3,4\}$ 到 $B=\{2,3,4\}$ 的关系，ρ_2 是一由 B 到 $C=\{1,2,3\}$ 的关系，其定义分别为

$$\rho_1=\{(a,b)\,|\,a+b=6\}=\{(2,4),(3,3),(4,2)\},$$

$$\rho_2=\{(b,c)\,|\,b-c=1\}=\{(2,1),(3,2),(4,3)\},$$

则由复合关系的定义 $\rho_1 \cdot \rho_2=\{(2,3),(4,1),(3,2)\}$。

作出各相应的关系矩阵，即

$$M_{\rho_1}=\begin{array}{c} \\ 1\\2\\3\\4\end{array}\begin{array}{c}\begin{array}{ccc}2&3&4\end{array}\\ \begin{pmatrix}0&0&0\\0&0&1\\0&1&0\\1&0&0\end{pmatrix}\end{array}; \qquad M_{\rho_2}=\begin{array}{c} \\ 2\\3\\4\end{array}\begin{array}{c}\begin{array}{ccc}1&2&3\end{array}\\ \begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}\end{array};$$

$$M_{\rho_1\rho_2}=\begin{array}{c} \\ 1\\2\\3\\4\end{array}\begin{array}{c}\begin{array}{ccc}1&2&3\end{array}\\ \begin{pmatrix}0&0&0\\0&0&1\\0&1&0\\1&0&0\end{pmatrix}\end{array}.$$

与例 1 比较可看出，这里的 M_{ρ_1}，M_{ρ_2} 分别就是例 1 中的 M_1，M_2，而 $M_{\rho_1\rho_2}=M_1 \cdot M_2$。因而有 $M_{\rho_1\rho_2}=M_{\rho_1} \cdot M_{\rho_2}$。这一结果并不偶然，实际上，对于复合关系的关系矩阵，我们有下面的定理。

定理 2-2 设 ρ_1 是一由 A 到 B 的关系，ρ_2 是一由 B 到 C 的关系（这里 A、B 和 C 都是有限集），它们的关系矩阵分别为 M_{ρ_1}，M_{ρ_2}，则复合关系 $\rho_1 \cdot \rho_2$ 的关系矩阵 $M_{\rho_1\rho_2}=M_{\rho_1} \cdot M_{\rho_2}$。

证明 设 $A=\{a_1,a_2,\cdots,a_l\}$, $B=\{b_1,b_2,\cdots,b_m\}$, $C=\{c_1,c_2,\cdots,c_n\}$, 又设 M_{ρ_1}, M_{ρ_2}, $M_{\rho_1\rho_2}$, $M_{\rho_1}\cdot M_{\rho_2}$ 的 (i,j) 通路分别为 $r_{ij}^{(1)}$, $r_{ij}^{(2)}$, r'_{ij}, r_{ij}。

由复合关系的定义，对于A与C中的任意两个元素 a_i 和 c_j，当且仅当存在某个 $b_k\in B$ 使得 $a_i\rho_1b_k$, $b_k\rho_2c_j$ 时，有 $a_i(\rho_1\cdot\rho_2)c_j$，反映在关系矩阵上，这也就是说，当且仅当存在某个 k $(1\leqslant k\leqslant m)$ 使得 $r_{ik}^{(1)}=1$ 且 $r_{kj}^{(2)}=1$ 时，有 $r'_{ij}=1$。另一方面，由关系矩阵乘积的定义可知，当且仅当存在某个 k $(1\leqslant k\leqslant m)$ 使得 $r_{ik}^{(1)}=1$ 且 $r_{kj}^{(2)}=1$ 时，有 $r_{ij}=\sum_{k=1}^{m}r_{ik}^{(1)}r_{kj}^{(2)}=1$。因此当且仅当 $r_{ij}=1$时，有 $r'_{ij}=1$。由 i, j 的任意性，故得 $M_{\rho_1\rho_2}=M_{\rho_1}\cdot M_{\rho_2}$。证完。

更一般地，我们可以得到下述的结论。

定理 2-3 设 ρ_1 是一由 A_1 到 A_2 的关系，ρ_2 是一由 A_2 到 A_3 的关系，$\cdots$，ρ_n 是一由 A_n 到 A_{n+1} 的关系（这里 $A_1,A_2,\cdots,A_{n+1}$ 都是有限集）。它们的关系矩阵分别是 $M_{\rho_1},M_{\rho_2},\cdots,M_{\rho_n}$，则复合关系 $\rho_1\rho_2\cdots\rho_n$（由 A_1 到 A_{n+1}）的关系矩阵 $M_{\rho_1\rho_2\cdots\rho_n}=M_{\rho_1}\cdot M_{\rho_2}\cdots M_{\rho_n}$。

此定理可根据定理 2-2 运用归纳法加以证明。

特别，当 $\rho_1=\rho_2=\cdots=\rho_n=\rho$, $A_1=A_2=\cdots=A_{n+1}=A$ 时，定理 2-3 又可简化为如下形式。

定理 2-4 设 ρ 是有限集 A 上的一个具有关系矩阵 M_ρ 的关系，则复合关系 ρ^n 的关系矩阵 $M_{\rho^n}=M_\rho^n$。

有限集A上的关系 ρ 的复合关系 ρ^n 仍为该有限集上的关系，因此它也可用关系图来表示。类似于关系矩阵，我们给出如何由 ρ 的关系图构造 ρ^n 的关系图的简单方法。

根据复合关系的定义，当且仅当在 A 中有 $a_{k_1},a_{k_2},\cdots,a_{k_{n-1}}$ 存在，使得 $a_i\rho a_{k_1},a_{k_1}\rho a_{k_2},\cdots,a_{k_{n-1}}\rho a_j$ 时，有 $a_i\rho^na_j$。因此，当且仅当在 ρ 的图中，有结点 $a_{k_1},a_{k_2},\cdots,a_{k_{n-1}}$，其边的指向由 a_i 到 a_{k_1}，

a_{k_1}到a_{k_2}，…，$a_{k_{n-1}}$到a_j时，则在ρ^n的图中，边由结点a_i指向a_j。于是，对于如何由ρ的关系图构造ρ^n的关系图，可按如下步骤进行：对于ρ的图中的每一个结点a_i，确定从a_i经由长为n的路能够到达的结点，这些结点就是在ρ^n的图中，边必须由结点a_i指向它们的那些结点。

例如，图2-4所表示的ρ^2和ρ^3的图，就是由图2-2所示的ρ的图按上述方法构成的。

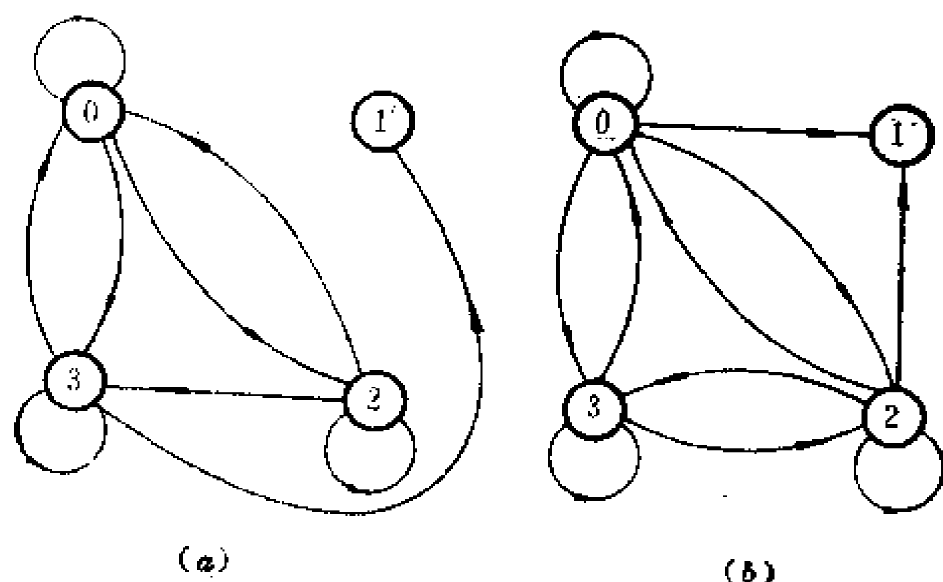


图2-4 $(a)\rho^2$的图，$(b)\rho^3$的图(对于图2-2的ρ)

下面，我们用关系的幂来构造称为**传递闭包**的新关系。关系的传递闭包在网络、语法分析以及开关电路中的故障检测和诊断等领域中，都有着重要的应用。

定义2.7 设ρ是集合A上的关系，则ρ的**传递闭包**用ρ^+表示，它是由下式定义的A上的关系，即

$$\rho^+ = \bigcup_{i=1}^{\infty} \rho^i .$$

当A为有限集时，笛卡尔积$A\times A$的基数$\#(A\times A)=(\#A)\times(\#A)=(\#A)^2$，因此$A\times A$的幂集$2^{A\times A}$的基数$\#(2^{A\times A})=$

$2^{\#(A\times A)}=2^{(\#A)^2}$，就是说 $A\times A$ 仅有 $2^{(\#A)^2}$ 个不同的子集。这就意味着集合 A 上仅有有限个不同的关系。因此，当 A 是有限集时，ρ 的传递闭包 ρ^+ 又可写为 $\rho^+=\bigcup_{i=1}^{m}\rho^i$（$m$ 为某正整数）。

于是，构造有限集上的关系 ρ 的传递闭包，其过程是有限的。例如我们由 ρ 逐步构造出 $\rho^2,\rho^3,\rho^4,\cdots$，这样继续下去，一定存在某个正整数 k，使得 $\rho^k=\rho^h(k>h)$。设 k 就是使得这一等式成立的最小正整数，则 $\rho^+=\bigcup_{i=1}^{k-1}\rho^i$。

事实上，若 $\#A=n$，则集合 A 上的传递闭包 $\rho^+=\bigcup_{i=1}^{n}\rho^i$。这一结论的证明请读者自己给出。

由定义 2-7，当且仅当存在某个正整数 k 使得 $a_i\rho^k a_j$ 时，有 $a_i\rho^+a_j$。就 ρ 的关系图而言，当且仅当 a_j 是从 a_i 经由任意有限长 k 的路能够到达时，有 $a_i\rho^k a_j$，因而有 $a_i\rho^+a_j$。因此由 ρ 的关系图可直接构造出 ρ^+ 的关系图：对于 ρ 的关系图中的每一个结点 a_i，找出从 a_i 经由有限长的路能够到达（即有路到达）的结点，这些结点就是在 ρ^+ 的关系图中边必须由结点 a_i 指向它们的那些结点。就关系矩阵而言，当且仅当存在某个关系矩阵 M_{ρ^k} 使得 $r_{ij}^{(k)}=1$ 时，ρ^+ 的关系矩阵 M_{ρ^+} 有 $r_{ij}^{(+)}=1$。于是，关系矩阵 M_{ρ^+} 的 (i,j) 通路可由关系矩阵 $M_\rho,M_{\rho^2},M_{\rho^3},\cdots,M_{\rho^n}$ 的 (i,j) 通路相加（布尔加）而得到，我们用符号写成

$$M_{\rho^+}=\sum_{i=1}^{n}M_{\rho^i}=\sum_{i=1}^{n}M_\rho^i,\quad(\#A=n).$$

例3 设 $A=\{1,2,3,4,5,6\}$ 上的关系 $\rho=\{(1,5),(4,3),(2,5),(4,5),(5,4),(6,3),(6,6)\}$，求 ρ 的传递闭包 ρ^+。

解 $\rho^2=\{(1,4),(2,4),(4,4),(5,5),(6,3),(6,6)\}$；

$\rho^3=\{(1,5),(2,5),(4,5),(5,4),(6,3),(6,6)\}$；

$\rho^4=\{(1,4),(2,4),(4,4),(5,5),(6,3),(6,6)\}$，

$\rho^4=\rho^2$。

所以 $\rho^+ = \rho \cup \rho^2 \cup \rho^3$

$= \{(1,3),(1,4),(1,5),(2,4),(2,5),(4,4),(4,5),(5,4),(5,5),(6,3),(6,6)\}$.

§2.5 关系的性质

定义在一个集合 A 上的关系 ρ 往往可以显出许多有用的性质。在此我们仅列出一些基本性质。

定义 2-8 设 ρ 是集合 A 上的关系，

(1) 若对于所有的 $a \in A$，有 $a\rho a$，则称 ρ 是**自反的**。否则 ρ **是非自反的**。

(2) 对于所有的 $a, b \in A$，若每当有 $a\rho b$ 就有 $b\rho a$，则称 ρ 是**对称的**。否则 ρ 是**非对称的**。

(3) 对于所有的 $a, b \in A$，若每当有 $a\rho b$ 和 $b\rho a$ 就必有 $a = b$，则称 ρ 是**反对称的**。

(4) 对于所有的 $a, b, c \in A$，若每当有 $a\rho b$ 和 $b\rho c$ 就有 $a\rho c$，则称 ρ 是**可传递的**。否则 ρ 是**不可传递的**。

注意区别自反关系和恒等关系，一个集合 A 上的恒等关系是自反关系，但自反关系却不一定是恒等关系。

实数集合 R 上的关系"$\leqslant$"是自反的、反对称的和可传递的。实数集上的关系"$<$"是非自反的、非对称的和可传递的。类似地，集合 2^U 上的包含关系"$\subseteq$"是自反的、反对称的和可传递的。真包含关系"$\subset$"是非自反的、非对称和可传递的。

在集合 2^U 上，若定义当且仅当 $S_i \cap S_j = \phi$ 时，有 $S_i \rho S_j$，则 ρ 是非自反的、对称的和不可传递的。若定义当且仅当 $S_i = S_j$ 时，有 $S_i \rho S_j$，则 ρ 是自反的、对称的且可传递的。

可以有这样的一种关系，它既是对称的又是反对称的。例如任何集合上的恒等关系就是这样的一种关系。

关系的这些性质，在关系矩阵和图上大多可以得到明确的反映：

若关系 ρ 是自反的，则 ρ 的关系图中的每一个结点引出一个单边环；若 ρ 是对称的，则在其关系图中，对每一由结点 a_i 指向结点 a_j 的边，必有一相反方向的边；若 ρ 是反对称的，则在其图中，任何两个不同的结点间最多只有一条边，而不会同时有两条相反方向的边；若 ρ 是可传递的，则若有由结点 a_i 指向 a_k 的边，且又有由结点 a_k 指向 a_j 的边，就必有一条由结点 a_i 指向 a_j 的边。

若关系 ρ 是自反的，则关系矩阵的主对角线上的元素全为 1；若 ρ 是对称的，则关系矩阵关于主对角线对称；若 ρ 是反对称的，则对 $i \neq j$，若 $r_{ij}=1$，则 $r_{ji}=0$。

当集合中元素的数目较大时，关系的图解表示和矩阵表达就变得不太方便了。然而在计算机上表达矩阵却不困难。根据关系矩阵，不难确定给定的关系是否是自反的或对称的，但根据关系矩阵确定给定的关系是否是可传递的，就不那么便当。

集合 A 上的关系 ρ 的传递闭包有如下性质。

定理 2-8 设 ρ 是集合 A 上的一个关系，则 ρ 的传递闭包 ρ^+ 是可传递的，且 ρ^+ 被包含于每一个包含 ρ 的可传递关系中。

证明 首先证明 ρ^+ 是可传递的。设有 $a\rho^+b$ 和 $b\rho^+c$，则必存在正整数 h 和 k，使得 $a\rho^h b$，$b\rho^k c$，由于关系的复合是可结合的，因此有 $a\rho^{h+k}c$，于是有 $a\rho^+c$，即 ρ^+ 是可传递的。

其次，设 $\bar{\rho}$ 是 A 上任意一个包含 ρ 的可传递关系，又设 $a\rho^+b$ 则由 ρ^+ 的定义，必存在有正整数 k，使得 $a\rho^k b$。因此必有元素 $b_1, b_2, \cdots, b_{k-1} \in A$，使得 $a\rho b_1, b_1\rho b_2, \cdots, b_{k-1}\rho b$，由于 $\rho \subseteq \bar{\rho}$，所以有 $a\bar{\rho}b_1, b_1\bar{\rho}b_2, \cdots, b_{k-1}\bar{\rho}b$，而 $\bar{\rho}$ 是可传递的，因此有 $a\bar{\rho}b$。由于 (a,b) 是 ρ^+ 的任意元素，故有 $\rho^+ \subseteq \bar{\rho}$。定理得证。

由此可知 ρ^+ 是包含 ρ 的最小可传递关系。类似地，我们定

义关系 ρ 的**自反闭包** $r(\rho)$ 为关系 $\rho \cup I_A$，**对称闭包** $S(\rho)$ 为关系 $\rho \cup \tilde{\rho}$。可以证明，$r(\rho)$ 是包含 ρ 的最小自反关系，而 $S(\rho)$ 是包含 ρ 的最小对称关系。显然，包含 ρ 的最小可传递且自反的关系由 $\rho^+ \cup I_A$ 给出，这个关系称为 ρ 的**自反传递闭包**，通常记为 ρ^*。

在下面的两小节里，我们将要介绍两种最有实际意义的关系，一种是自反、对称、可传递的关系，称为等价关系。另一种是自反、反对称、可传递的关系，称为偏序关系。相容关系将在习题中由读者来完成对它的讨论。

§2.6 等价关系

定义 2-9 集合 A 上的关系 ρ，如果它是自反、对称且可传递的，则称 ρ 为 A 上的**等价关系**。也就是说，具有以下性质的关系 ρ 称为等价关系。

(1) 对所有的 $a \in A$，有 $a\rho a$；

(2) 对所有的 $a, b \in A$，若有 $a\rho b$，则有 $b\rho a$；

(3) 对所有的 $a, b, c \in A$，若有 $a\rho b$ 和 $b\rho c$，则有 $a\rho c$。

最熟悉的等价关系是一个集合的元素之间的相等关系。又如平面几何中的直线之间的平行关系、三角形的相似关系、在给定的城市中"住在同一条街上"的居民之间的关系等都是等价关系。

设 ρ 是 A 上的等价关系，若 $a\rho b$ 成立，则我们说 a 等价于 b（在 ρ 下）。如果 a 等价于 b，则因为 ρ 是对称的，b 也等价于 a。因此，如果有 $a\rho b$，则我们可以简单地说 a 和 b 是等价的（在 ρ 下）。

定义 2-10 设 ρ 是集合 A 上的等价关系，则 A 中等价于 a 的全体元素的集合称为 a 所生成的**等价类**，用 $[a]_\rho$ 表示，即

$$[a]_\rho = \{b \mid b \in A, a\rho b\}.$$

当集合 A 上仅定义了等价关系 ρ 时，则常将 $[a]_\rho$ 简记成 $[a]$。

现在我们来看看由A中元素所生成的等价类的一些性质：

1．对于任意元素$a\in A$，有$a\rho a$，因此$a\in[a]_\rho$，即A中每一元素所生成的等价类非空。

2．若$a\rho b$，则$[a]_\rho=[b]_\rho$。这就是说，彼此等价的元素属于同一个等价类。这是因为，若$x\in[a]_\rho$，则$a\rho x$；又因为$a\rho b$，由ρ的对称性和传递性有$b\rho x$，于是，有$x\in[b]_\rho$，因此$[a]_\rho\subseteq[b]_\rho$。类似地，也有$[b]_\rho\subseteq[a]_\rho$，故$[a]_\rho=[b]_\rho$。

3．若$a\rho' b$，则$[a]_\rho\cap[b]_\rho=\phi$。这就是说，彼此不等价的元素属于不同的等价类，而且这些等价类之间没有公共元素。这是因为，如果有元素$x\in[a]_\rho\cap[b]_\rho$，则$a\rho x$且$b\rho x$，从而$a\rho b$，这与假设$a\rho' b$相矛盾。

由等价类的这些性质，我们可得到下面的定理。

定理 2-6　设ρ是集合A上的等价关系，则等价类的集合$\{[a]_\rho|a\in A\}$构成A的一个分划。

证明　由前述等价类的性质可知，对任意的$a\in A$，$[a]_\rho$非空。又任意两个等价类$[a]_\rho$和$[b]_\rho$，或者就是同一个等价类，或者$[a]_\rho\cap[b]_\rho=\phi$。剩下只要证明$\bigcup_{a\in A}[a]_\rho=A$。显然，$\bigcup_{a\in A}[a]_\rho\subseteq A$。对任意的元素$c\in A$，有$c\in[c]_\rho$，而$[c]_\rho\subseteq\bigcup_{a\in A}[a]_\rho$，因此$c\in\bigcup_{a\in A}[a]_\rho$，从而$A\subseteq\bigcup_{a\in A}[a]_\rho$，故有$\bigcup_{a\in A}[a]_\rho=A$。

由上可知，等价类的集合$\{[a]_\rho|a\in A\}$构成A的一个分划，定理得证。

定理 2-6 说明，集合A上任意一个等价关系ρ定义A的一个分划，每一个等价类就是一个分划块。因为A的每一元素的等价类（在ρ下）是唯一的，所以这样的分划也是唯一的。我们把这种由等价关系ρ的等价类所组成的A的分划，称为A上由ρ所导出的等价分划，用π_ρ^A表示。

例 1 $A=\{0,1,2,3,4,5\}$上的关系

$$\rho=\{(0,0),(1,1),(2,2),(3,3),(1,2),(1,3),(2,1),(2,3),(3,1),(3,2),(4,4),(4,5),(5,4),(5,5)\}. \qquad (1)$$

ρ的关系图由图 2-5 给出。由图可见ρ是自反的、对称的和可传递的，因此是一等价关系，它在A上所导出的等价分划

$$\pi_A^\rho=\{[0],[1],[4]\}=\{\{0\},\{1,2,3\},\{4,5\}\}. \qquad (2)$$

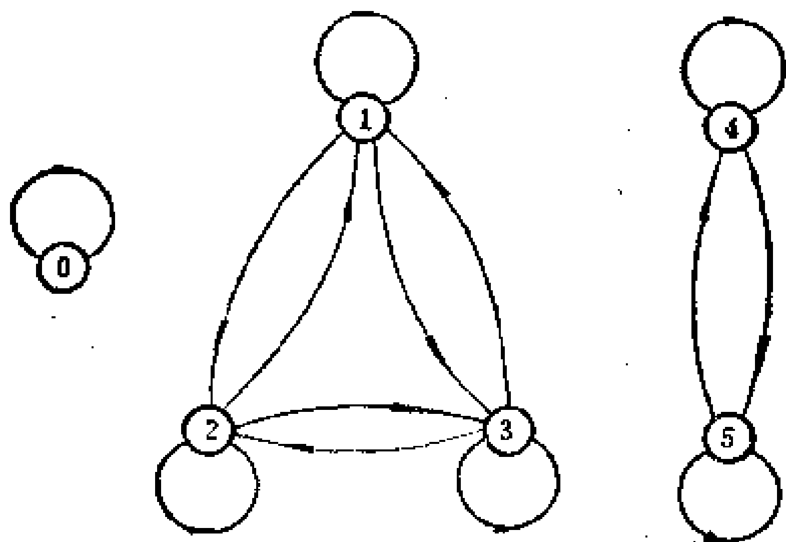


图 2-5 例1的关系图

给出等价关系ρ（如(1)式），根据定理 2-6，我们可以得到等价分划π_A^ρ（如(2)式）。反之，若给定某等价分划π_A^ρ，则我们根据同一等价类中元素都相互等价，不同等价类的元素都互不等价，可将凡属同一等价类中的元素所形成的所有可能的对偶列出，便得到等价关系ρ。因此π_A^ρ是ρ的另一种形式的表示方法。借助π_A^ρ来表示等价关系ρ，通常比列出其全部对偶的办法来得更简洁明了。

对于任何集合A，恒等关系I_A和普遍关系U_A都是等价关系。在由I_A所导出的等价分划中，每一等价类仅由一个元素组成，这显然是集合A的"最细"的分划。在由U_A所导出的等价

分划中，只有由A的全部元素组成的一个等价类，这是集合A的“最粗”的分划，这些分划有时被称为A的**平凡分划**。

定义 2-11 设ρ是集合A上的等价关系，则等价类的集合$\{[a]_\rho | a \in A\}$称为A关于ρ的**商集**，用A/ρ表示。A/ρ的基数(即A在ρ下的不同等价类的个数）称为ρ的**秩**。

所谓集合A关于ρ的商集就是ρ在A上所导出的等价分划。

例 1 中A关于ρ的商集$A/\rho = \{[0], [1], [4]\}$。

对于任何整数i和正整数m，我们用$\mathrm{res}_m(i)$表示用m除i所得的余数。显然，对于给定的i和m，$\mathrm{res}_m(i)$是唯一确定的，且$0 \leqslant \mathrm{res}_m(i) < m$（参见§3.8）。对于任意两个整数$i_1$和$i_2$，如果$\mathrm{res}_m(i_1) = \mathrm{res}_m(i_2)$，则我们说$i_1$和$i_2$“模$m$相等”或“模$m$同余”，写成：$i_1 \equiv i_2 (\mathrm{mod}\ m)$。设$i_1 = q_1 m + \mathrm{res}_m(i_1)$，$i_2 = q_2 m + \mathrm{res}_m(i_2)$，则$\mathrm{res}_m(i_1) = i_1 - q_1 m$，$\mathrm{res}_m(i_2) = i_2 - q_2 m$。因此，当且仅当$i_1 - q_1 m = i_2 - q_2 m$，也就是当且仅当$i_1 - i_2 = (q_1 - q_2) m$时，有$\mathrm{res}_m(i_1) = \mathrm{res}_m(i_2)$，即当且仅当$i_1 - i_2$是$m$的整数倍时，$i_1 \equiv i_2 (\mathrm{mod}\ m)$。

例 2 设ρ是整数集I上的关系，定义为当且仅当$i_1 \equiv i_2 (\mathrm{mod}\ 3)$时，有$i_1 \rho i_2$（即$\rho$是“模 3 同余”关系）。因为$i_1 - i_1 = 0 \cdot 3$，所以$\rho$是自反的。又因为若$i_1 - i_2 = q \cdot 3$，则$i_2 - i_1 = (-q) \cdot 3$，所以$\rho$是对称的。最后，若$i_1 - i_2 = q \cdot 3$，$i_2 - i_3 = p \cdot 3$，则$i_1 - i_3 = (i_1 - i_2) + (i_2 - i_3) = (q + p) \cdot 3$。所以$\rho$是可传递的。因此，$\rho$是一个等价关系。$\rho$在$I$上的所有等价类构成$I$的一个等价分划

$$\pi_\rho^I = \{[0]_\rho, [1]_\rho, [2]_\rho\},$$

故I关于ρ的商集

$$I/\rho = \{[0]_\rho, [1]_\rho, [2]_\rho\},$$

其中
$$[0]_\rho = \{\cdots, -6, -3, 0, 3, 6, \cdots\};$$
$$[1]_\rho = \{\cdots, -5, -2, 1, 4, 7, \cdots\};$$
$$[2]_\rho = \{\cdots, -4, -1, 2, 5, 8, \cdots\}.$$

显然，对于任意正整数m，"模m同余"关系都是整数集 I 上的等价关系。

由定理 2-6 可知，集 A 上每一等价关系定义 A 上的一个分划。反之，若给定集合A上一个分划，是否可确定A上一等价关系呢？回答是肯定的。

定理 2-7 设 $\pi=\{A_i\}_{i\in k}$ 是集合A的一个分划，则存在一个A上的等价关系ρ，使得π是A上由ρ导出的等价分划。

证明 定义A上的关系ρ为当且仅当a和b属于π的同一分划块A_i时，有$a\rho b$，显然，ρ是一个等价关系，且每一等价类就是一个分划块。证完。

由定理 2-6 和定理 2-7 可知，"分划"的概念和"等价关系"的概念，在本质上是相同的。

例 3 设集合 $A=\{a,b,c,d\}$，A的一分划$\pi=\{\{a,b\},\{c\},\{d\}\}$，则相应的等价关系$\rho=\{(a,a),(b,b),(a,b),(b,a),(c,c),(d,d)\}$。

§2.7 偏 序

定义 2-12 集合A上的一个关系ρ，如果它是自反、反对称和可传递的，即

(1) 对所有的$a\in A$，有$a\rho a$；

(2) 对所有的$a,b\in A$，若$a\rho b$且$b\rho a$，就必有$a=b$；

(3) 对所有的$a,b,c\in A$，若$a\rho b$且$b\rho c$，就必有$a\rho c$。

则称ρ是A上的一个**偏序关系**，或简称为**偏序**。偏序通常用符号"$\leqslant$"表示。

显然，一个偏序的逆也是一个偏序。通常用符号"$\geqslant$"表示。

下面给出偏序的两个重要的特殊情形。

定义 2-13 一个集合A上的偏序，若对于所有的$a,b\in A$，有$a\leqslant b$或$b\leqslant a$，则称它为A上的一个**全序**。

定义 2-14 一个集合 A 上的偏序，若对于 A 的每一个非空子集 $S\subseteq A$，在 S 中存在一个元素 a_s（称为 S 的最小元素），使得对于所有的 $s\in S$，有 $a_s\leqslant s$，则称它为 A 上的一个**良序**。

例 1 定义在实数集 R 上的"小于或等于"关系 $\leqslant$，是 R 上的偏序关系。实际上，表示偏序的符号"$\leqslant$"就是从此特例中借用来的，以表示更为普遍的偏序关系。

例 1 中的关系也是 R 上的一个全序，但它不是 R 上的良序，例如，开区间 $(0,1)$ 是 R 的子集，但 $(0,1)$ 中没有最小元素。

例 2 定义在正整数集 N 上的"小于或等于"关系 $\leqslant$ 是 N 上的偏序关系，也是 N 上的全序和良序。

例 3 定义在正整数集 N 上的整除关系（对于任意 $n_1,n_2\in N$，当且仅当存在一个整数 m，使得 $n_1m=n_2$，则称"n_1 整除 n_2"，记为 $n_1|n_2$。）是一个偏序，但不是全序，也不是良序。因为，显然对于 $3,5\in N$，既没有 $3|5$，也没有 $5|3$，所以不是全序。由此可知，对于 N 的子集 $\{3,5\}$ 没有最小元素，因此也不是良序。

容易验证，以上例中的逆关系也都是相应集合上的偏序关系。

实数集 R 上的小于关系"$<$"和大于关系"$>$"都不是偏序关系，因为它们都不是自反的。

设 $\leqslant$ 是集合 A 上的偏序关系，对于任意 $a,b\in A$，如果有 $a\leqslant b$ 或 $b\leqslant a$，则元素 a 和 b 称为是**可比的**，否则称 a 和 b 是**不可比的**。如例 3 中的 3 和 5 就是不可比的。然而，对于集合 A 上的任一全序，集合 A 中任意两个元素都是可比的。

例 4 设 $A=\{a, b, c\}$，幂集 2^A 上的包含关系，即当且仅当 $S_1\subseteq S_2$ 时，有 $S_1\rho S_2$，显然是自反，反对称和可传递的。因此是 2^A 上的一个偏序。但由于 $\{a\}$ 和 $\{b,c\}$，$\{a,b\}$ 和 $\{a,c\}$ 等是不可比的，故它不是全序。

由定义，一个集合 A 上的全序或良序一定是偏序，然而偏序却不一定是全序或良序。一个偏序若是良序，则一定也是全序。

这是因为对于集合A的任何子集，譬如说$\{a,b\}$，我们必定有a或b作它的最小元素。然而一个全序却不一定是良序，但若是有限集上的全序，则一定是良序。

全序的一个有用的例子是词典编辑次序。

例 5　设L表示一字母集（比如26个英文字母），在其上定义了一个全序$\leqslant$（如通常的字母顺序，$A\leqslant B\leqslant C\leqslant D\cdots\leqslant Z$），$\bar{L}$表示由$L$中的元素构成的全部词的集合，则可如下定义$\bar{L}$上的关系$\rho$，对于$\bar{L}$中的任意两个元素$u_1u_2\cdots u_h$和$v_1v_2\cdots v_k$其中$h\leqslant k$（如果$h\leqslant k$不成立，可交换这两个词以便使得$h\leqslant k$），如果下述条件中的任何一个成立：

(1) $u_1=v_1$，$u_2=v_2$，$\cdots$，$u_h=v_h$；

(2) $u_1\neq v_1$且在L中$u_1\leqslant v_1$；

(3) 对于某正整数r $(1\leqslant r<h)$，有$u_1=v_1$，$u_2=v_2$，$\cdots$，$u_r=v_r$和$u_{r+1}\neq v_{r+1}$以及在L中$u_{r+1}\leqslant v_{r+1}$，

则
$$(u_1u_2\cdots u_h)\rho(v_1v_2\cdots v_k).$$

如果这些条件中没有任何一个满足，则
$$(v_1v_2\cdots v_k)\ \rho\ (u_1u_2\cdots u_h).$$

可以证明，ρ是$\bar{L}$上的一个全序。

在英语词典中，词出现的顺序就是词典偏序的一个熟悉的例子。例如

compute ρ *computer*（由条件(1)），

eleven ρ *relation*（由条件(2)），

compute ρ *comrade*（由条件(3)），

get ρ *go*（由最后的规则）。

上述词典编辑次序还可推广到一般。设$\leqslant$是集合A上的全序，并设集合$X=A\cup A^2\cup A^3\cup\cdots\cup A^n$（$n$为某一正整数），即$X$是由长度小于或等于$n$的元素串所组成。于是，可以按照例5给出的三个条件，定义X中的全序关系ρ。

无疑可以用前面讨论过的关系图来表示有限集A上的偏序关系。然而通常是使用更为简便的**次序图**（或称 *Hasse* 图）来表示它。这种图有$\#A$个结点，每一个结点代表A的一个元素，并画作一个带有元素标号的小圆圈。若结点$a\neq b$且$a\leqslant b$，则结点a出现在结点b的下面。边连接这样的两个结点a和b：$a\neq b$，$a\leqslant b$，且不存在任何其它元素c，使得$a\leqslant c\leqslant b$（对此情形有时称元素b复盖a）。因此在次序图中，当且仅当$a=b$或者从b经由一条下降的路可以到达a时，有$a\leqslant b$成立。这样，所有的边的方向都是自下朝上，故可略去边上的全部箭头表示。

例6 $J=\{2,3,4,6,8,12,36,60\}$上的整除关系$|$是一个偏序，图2-6给出了该偏序的次序图。

例7 定义在全集合U的幂集上的包含关系$\subseteq$是一个偏序。设$U=\{a, b, c\}$，则该偏序的次序图由图2-7给出。

例8 设$A=\{1, 2, 3, 4\}$，$\leqslant$是"小于或等于"关系，则$\leqslant$是集合A上的一个全序。其次序图由图2-8给出。

显然，全序的次序图仅由一条竖直边上结点的序列组成。

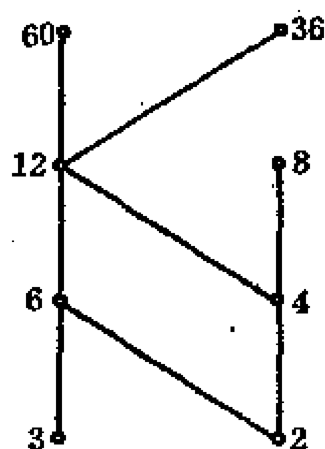


图2-6

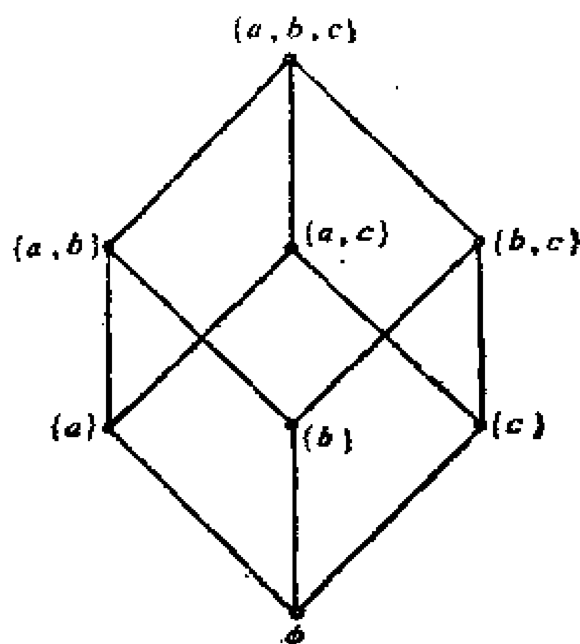


图2-7

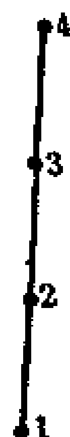


图2-8

习　题

1. 若 $A=\{0,1\}$、$B=\{1,2\}$，确定集合

(1) $A\times\{1\}\times B$；　　(2) $A^2\times B$；　　(3) $(B\times A)^2$。

2. 在通常的具有 X 轴和 Y 轴的笛卡尔坐标系中，若有

$$X=\{x \mid x\in R,\ -3\leqslant x\leqslant 2\};$$

$$Y=\{y \mid y\in R,\ -2\leqslant y\leqslant 0\},$$

试给出笛卡尔积 $X\times Y$ 的几何解释。

3. 对任何集合 A、B 和 C，证明：

(1) $A\times(B\cup C)=(A\times B)\cup(A\times C)$；

(2) $A\times(B\cap C)=(A\times B)\cap(A\times C)$。

4. 设 A，B 和 C 是任意三个集合，证明：

$$(A\cap B)\times(C\cap D)=(A\times C)\cap(B\times D).$$

5. 对下列每种情形，列出由 A 到 B 的关系 ρ 的元素，确定 ρ 的定义域和值域，构造 ρ 的关系矩阵：

(1) $A=\{0,1,2\}$，$B=\{0,2,4\}$，$\rho=\{(a,b) \mid ab\in A\cap B\}$；

(2) $A=\{1,2,3,4,5\}$，$B=\{1,2,3\}$，$\rho=\{(a,b) \mid a=b^2\}$；

(3) $A=2^{\{0,1\}}$，$B=2^{\{0,1,2\}}-2^{\{0\}}$，$\rho=\{(a,b) \mid a-b=\phi\}$。

6. 设 $A=\{1,2,3,4,5,6\}$，对下列每一种情形，构造 A 上的关系 ρ 的关系图，并确定 ρ 的定义域和值域：

(1) $\rho=\{(i,j) \mid i=j\}$；

(2) $\rho=\{(i,j) \mid i$ 整除 $j\}$；

(3) $\rho=\{(i,j) \mid i$ 是 j 的倍数$\}$；

(4) $\rho=\{(i,j) \mid i>j\}$；

(5) $\rho=\{(i,j) \mid i<j\}$；

(6) $\rho=\{(i,j) \mid i\neq j,\ ij<10\}$；

(7) $\rho=\{(i,j) \mid (i-j)^2\in A\}$；

(8) $\rho=\{(i,j) \mid i/j$ 是素数$\}$。

7. 设 $\rho_1=\{(1,2),(2,4),(3,3)\}$ 和 $\rho_2=\{(1,3),(2,4),(4,2)\}$，试求出 $\rho_1\cup\rho_2$，$\rho_1\cap\rho_2$，D_{ρ_1}，D_{ρ_2}，$D_{(\rho_1\cup\rho_2)}$，R_{ρ_1}，R_{ρ_2} 和 $R_{(\rho_1\cap\rho_2)}$，并证明：

$$D_{(\rho_1\cup\rho_2)}=D_{\rho_1}\cup D_{\rho_2};\quad R_{(\rho_1\cap\rho_2)}\subseteq R_{\rho_1}\cap R_{\rho_2}.$$

8. A_1 和 A_2 是分别具有基数 n_1 和 n_2 的有限集，试问有多少个由 A_1 到 A_2 的不同关系？

9. 指出集合 $A=\{a_1,a_2,\cdots,a_n\}$ 上的普遍关系和恒等关系的关系矩阵和关系图的特征.

10. 下列是集合 $A=\{0,1,2,3\}$ 上的关系：

$$\rho_1=\{(i,j)\mid j=i+1 \text{ 或 } j=i/2\};$$
$$\rho_2=\{(i,j)\mid i=j+2\}.$$

试确定如下的复合关系：

(1) $\rho_1\cdot\rho_2$；(2) $\rho_2\cdot\rho_1$；(3) $\rho_1\cdot\rho_2\cdot\rho_1$；(4) ρ_1^3.

11. 设 ρ_1,ρ_2,ρ_3 是集合 A 上的关系，试证明如果 $\rho_1\subseteq\rho_2$，则有

(1) $\rho_1\cdot\rho_3\subseteq\rho_2\cdot\rho_3$；(2) $\rho_3\cdot\rho_1\subseteq\rho_3\cdot\rho_2$；(3) $\tilde{\rho}_1\subseteq\tilde{\rho}_2$.

12. 给定 $\rho_1=\{(0,1),(1,2),(3,4)\}$，

$$\rho_1\cdot\rho_2=\{(1,3),(1,4),(3,3)\},$$

求一个基数最小的关系，使满足 ρ_2 的条件。一般地说，若给定 ρ_1 和 $\rho_1\cdot\rho_2$，ρ_2 能被唯一地确定吗？基数最小的 ρ_2 能被唯一地确定吗？

13. 给定集合 A_1，A_2，A_3，设 ρ_1 是由 A_1 到 A_2 的关系，ρ_2 和 ρ_3 是由 A_2 到 A_3 的关系，试证明：

(1) $\rho_1\cdot(\rho_2\cup\rho_3)=(\rho_1\cdot\rho_2)\cup(\rho_1\cdot\rho_3)$；

(2) $\rho_1\cdot(\rho_2\cap\rho_3)\subseteq(\rho_1\cdot\rho_2)\cap(\rho_1\cdot\rho_3)$.

14. 给定 $\rho=\{(i,j)\mid i,j\in I,\ j-i=1\}$，$\rho^n$ 是什么？

15. 对第10题中的关系，构造关系矩阵：

(1) M_{ρ_1}；(2) M_{ρ_2}；(3) $M_{\rho_1\cdot\rho_2}$；

(4) $M_{\rho_2\cdot\rho_1}$；(5) $M_{\rho_1\cdot\rho_2\cdot\rho_1}$；(6) $M_{\rho_1^3}$.

16. 设ρ_1是由A到B的关系，ρ_2是由B到C的关系。试证明$\widetilde{\rho_1\cdot\rho_2}=\tilde{\rho}_2\cdot\tilde{\rho}_1$。

17. (1) 设ρ_1和ρ_2是由A到B的关系，问$\widetilde{\rho_1\cup\rho_2}=\tilde{\rho}_1\cup\tilde{\rho}_2$成立吗?

(2) 设ρ是集合A上的关系，如果ρ是自反的，则$\tilde{\rho}$一定是自反的吗?如果ρ是对称的，则$\tilde{\rho}$一定是对称的吗?如果ρ是可传递的，则$\tilde{\rho}$一定是可传递的吗?

18. 图2-9给出了集合$\{1,2,3,4,5,6\}$上的关系ρ的关系图，试画出关系ρ^5和ρ^8的图，并利用关系图求出关系ρ的传递闭包。

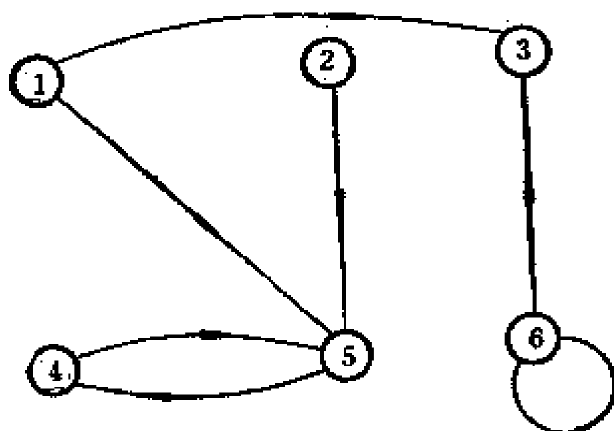


图 2-9

19. 试证明：若ρ是基数为n的集合A上的一个关系，则ρ的传递闭包为$\rho^+=\bigcup_{i=1}^{n}\rho^i$.

20. 下列关系中哪一个是自反的、对称的或可传递的?

(1) 当且仅当$|i_1-i_2|\leqslant 10\ (i_1,i_2\in I)$时，有$i_1\rho i_2$;

(2) 当且仅当$n_1 n_2>8\ (n_1,n_2\in N)$时，有$n_1\rho n_2$;

(3) 当且仅当$r_1\leqslant|r_2|\ (r_1,r_2\in R)$时，有$r_1\rho r_2$.

21. 设ρ_1和ρ_2是集合A上的任意两个关系. 判断下列命题是否正确，并说明理由。

(1) 若ρ_1和ρ_2是自反的，则$\rho_1\cdot\rho_2$也是自反的.

(2) 若ρ_1和ρ_2是非自反的，则$\rho_1\cdot\rho_2$也是非自反的.

(3) 若 ρ_1 和 ρ_2 是对称的，则 $\rho_1 \cdot \rho_2$ 也是对称的。

(4) 若 ρ_1 和 ρ_2 是反对称的，则 $\rho_1 \cdot \rho_2$ 也是反对称的。

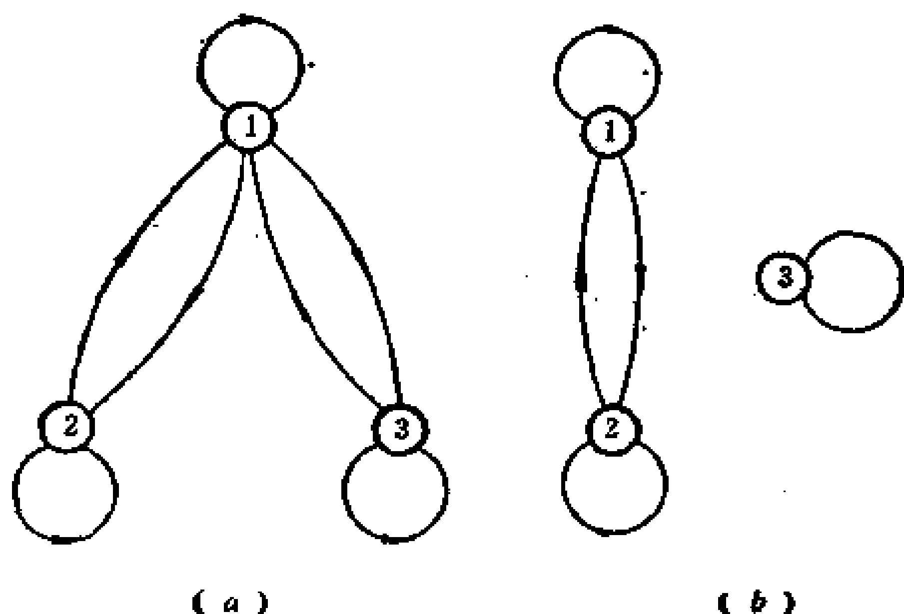
(5) 若 ρ_1 和 ρ_2 是可传递的，则 $\rho_1 \cdot \rho_2$ 也是可传递的。

22. 试证明：若关系 ρ 是对称的，则 ρ^k（对任何整数 $k \geq 1$）也是对称的。

23. 已给 $A = \{1,2,3,4\}$ 和定义在 A 上的关系 $\rho = \{(1,2),(4,3),(2,2),(2,1),(3,1)\}$。证明 ρ 不是可传递的。求出一个关系 $\rho_1 \supseteq \rho$，使得 ρ_1 是可传递的。你能求出另一个关系 $\rho_2 \supseteq \rho$ 也是可传递的吗？

24. 图 2-10 表示在 $\{1,2,3\}$ 上的 12 个关系的关系图。试对每一个这样的图，确定其表示的关系是自反的还是非自反的；是对称，非对称还是反对称的；是可传递的还是不可传递的。

25. 图 2-11 给出了 $\{1,2,3\}$ 上两个关系的关系图，这些关系是等价的吗？



(a)　　(b)

图 2-11

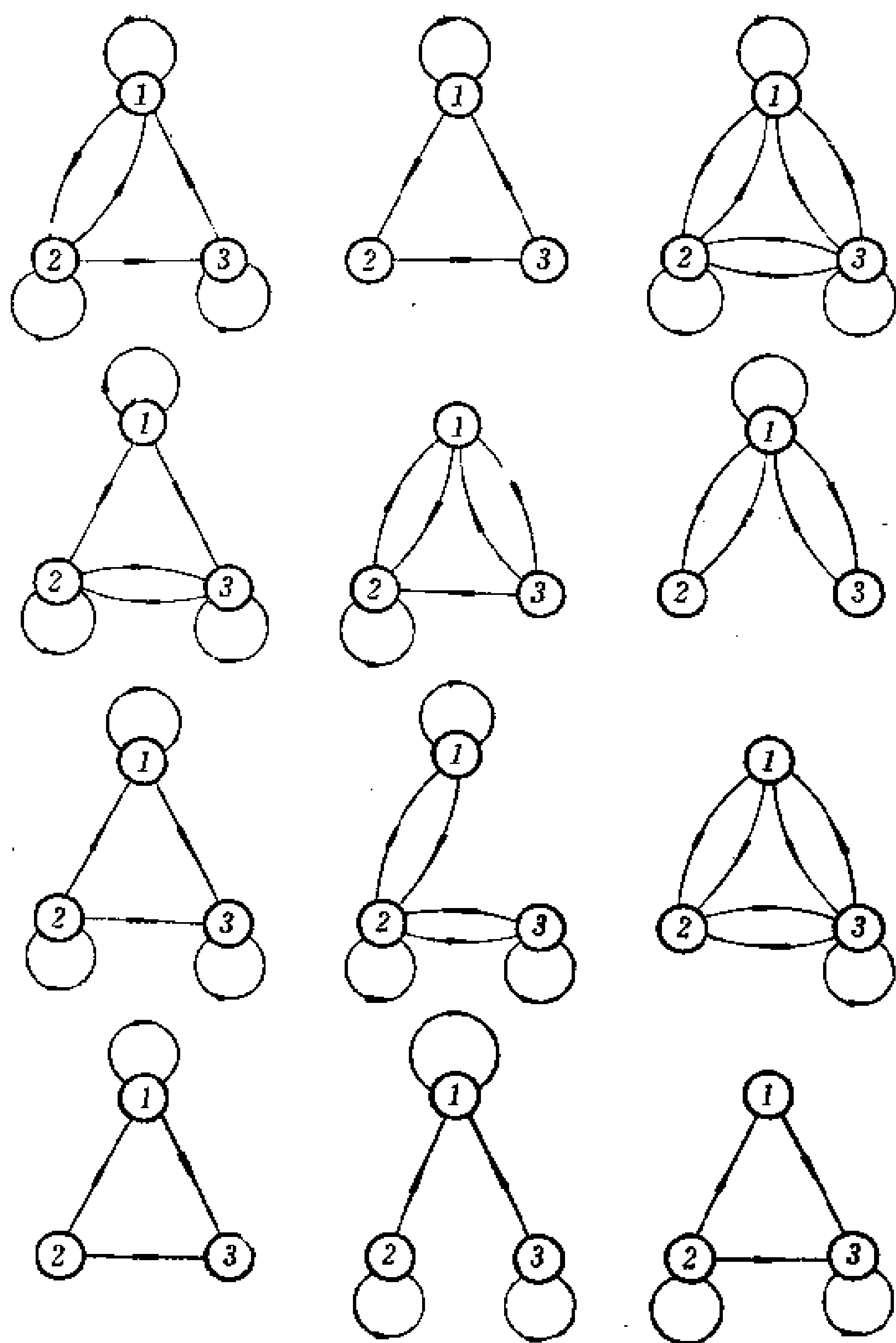


图 2-10

26. 在N上的关系ρ定义为当且仅当n_i/n_j可以用形式2^m表示时，有$n_i \rho n_j$。这里m是任意整数。

(1) 证明ρ是等价关系。　　(2) 找出ρ的所有等价类。

27. 有人说，集合A上的关系ρ，如果是对称的且可传递的，则它也是自反的，其理由是，从$a_i \rho a_j$，由对称性得$a_j \rho a_i$，再由可传递性使得$a_i \rho a_i$。你的意见如何？

28. 设有集合A和A上的关系ρ，对于所有的a_i、a_j、$a_k \in A$，若由$a_i \rho a_j$和$a_j \rho a_k$可推得$a_k \rho a_i$，则称关系ρ是循环的。试证明当且仅当ρ是等价关系时，ρ是自反且循环的。

29. 设ρ_1和ρ_2是A上的等价关系，试证明：当且仅当$\pi_{\rho_1}^A$中的每一等价类都包含于$\pi_{\rho_2}^A$的某一等价类中时，有$\rho_1 \subseteq \rho_2$。

30. 已知ρ_1和ρ_2是集合A上分别有秩r_1和r_2的等价关系，试证明$\rho_1 \cap \rho_2$也是A上的等价关系，它的秩至多为$r_1 r_2$。再证明$\rho_1 \cup \rho_2$不一定是A上的等价关系。

31. 设ρ_1是集合A上的一个关系，$\rho_2 = \{(a,b) \mid$ 存在c，使$(a,c) \in \rho_1$且$(c,b) \in \rho_1\}$。证明：若ρ_1是一个等价关系，则ρ_2也是一个等价关系。

32. 设ρ是集合A上的一个等价关系，而$\{A_1, A_2, \cdots, A_k\}$是$A$的子集的集合，当$i \neq j$时，$A_i \nsubseteq A_j$，且使得当且仅当$a$和$b$在同一个子集中时，有$a \rho b$，证明$\{A_1, A_2, \cdots, A_k\}$是$A$的一个分划。

33. 对于下列集合中的“整除”关系，画出次序图。

(1) {1, 2, 3, 4, 6, 8, 12, 24}；

(2) {1,2,3,4,5,6,7,8,9,10,11,12}。

34. 对于下列集合，画出偏序关系“整除”的次序图，并指出哪些是全序。

(1) {2,6,24}；　　(2) {3,5,15}；

(3) {1,2,3,6,12}；　　(4) {2,4,8,16}；

(5) {3,9,27,54}。

35. 如果 ρ 是集合 A 中的偏序关系，且 $B\subseteq A$，试证明：$\rho\cap(B\times B)$ 是 B 上的偏序关系。

36. 给出一个集合 A 的例子，使得包含关系 $\subseteq$ 是幂集 2^A 上的一个全序。

37. 给出一个关系，使它既是某一集合上的偏序关系又是等价关系。

38. 图 2-12 表示 $\{1,2,3,4\}$ 上的四个偏序的关系图。画出每一个的次序图，并指出其中哪些是全序，哪些是良序。

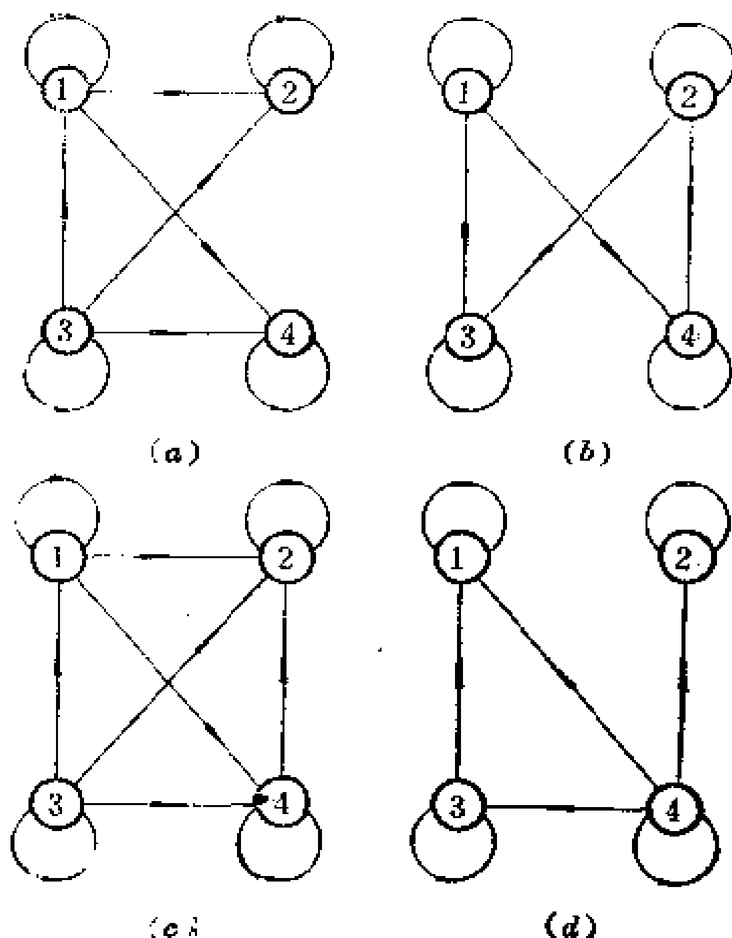


图 2-12

39. 一个集合上的自反和对称的关系称为相容关系。

(1) 设 A 是人的集合，ρ 是 A 上的关系，定义为当且仅当 a 是 b 的朋友时，有 $a\rho b$。证明 ρ 是 A 上的相容关系。

(2) 设 ρ 是正整数集 N 上的关系，当且仅当两个正整数 n_1 和 n_2 中有相同的数字时，$n_1\rho n_2$。证明 ρ 是一个相容关系。

(3) 再举出一个相容关系的例子。

(4) 设 ρ_1 和 ρ_2 是 A 上的两个相容关系，$\rho_1\cap\rho_2$ 是相容关系吗？$\rho_1\cup\rho_2$ 是相容关系吗？

40. 设 A 是一个集合，A 的一个覆盖是 A 的一个非空子集的集合 $\{A_1,A_2,\cdots,A_k\}$，它使得 $\bigcup_{i=1}^{k}A_i=A$，

(1) 给出一种由A的一个覆盖定义A上的一个相容关系的方法。

(2) $S=\{\{a_1,a_2,a_4\},\ \{a_2,a_3,a_5\},\ \{a_2,a_4,a_5\}\}$是集合$A=\{a_1,a_2,a_3,a_4,a_5\}$上的一个覆盖。试定义$A$上的一个相容关系。

41. 设有集合A，ρ是A上的相容关系。如果$A_i\subseteq A$，并且满足：

(a) A_i中任一元素a与A_i中所有的元素都有相容关系ρ；

(b) $A-A_i$中没有能与A_i中所有元素都有相容关系ρ的元素，

则称子集A_i为最大相容类。

(1) 图2-13和图2-14分别给出了集合$A=\{1,2,3,4,5,6\}$上的相容关系ρ_1和ρ_2的关系图的简图（图中省略了由每一结点引出的单边环，并将两结点间方向相反的两条边用一条无向边代替）。试由这些图确定其相应的所有最大相容类。

(2) 试给出由相容关系的关系图求其最大相容类的一般方法。

(3) 如何由集合A上定义的一个相容关系ρ来定义A的一个覆盖？

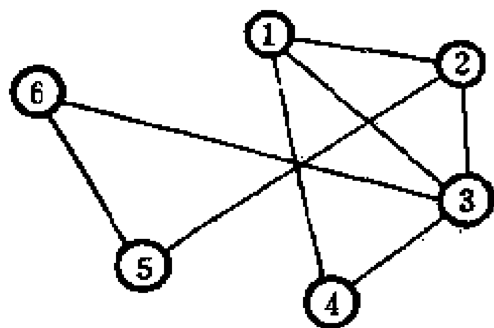


图 2-13

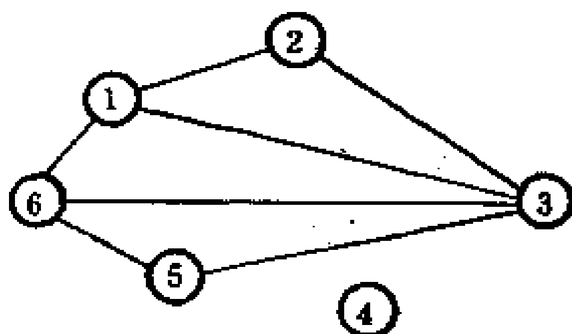


图 2-14

第三章 函 数

这一章我们介绍函数的概念。函数是一种特殊的关系。在引入一般的函数概念之后，进一步研究三种特殊的函数：内射、满射和双射。类似于关系，定义复合函数、恒等函数和逆函数。在整个计算机科学的理论研究中，数学归纳法是一种极为重要的方法，因此本章介绍了数学归纳法。在这一章的末尾，我们还讨论了整数的一些最基本的性质。因为这些性质对于研究计算机内的数字表示和算术运算有重要的意义，而且它们与数字系统中的误差检测和校正也是有关的。

与集合和关系的概念一样，函数的概念对于计算机科学工作者来说也是必不可少的。它直接应用到诸如开关理论、自动机理论和可计算性等领域中。

§3.1 函 数

上一章我们曾详细讨论了定义在两个集合上的二元关系。我们知道，关系是一个意义相当广泛的概念，它没有对两个集合的元素作任何特殊的限制，而只要是笛卡尔积 $A\times B$ 的子集，便可形成一由 A 到 B 的关系。

定义 3-1 设有集合 A、B，f 是一由 A 到 B 的关系，如果对于每个 $a\in A$，存在唯一的 $b\in B$ 使得 afb，则称关系 f 是由 A 到 B 的一个**函数**，记为 $f: A\to B$。

显然，f 的**定义域** $D_f=A$，f 的**值域** $R_f\subseteq B$。我们称 B 为 f 的**值域包**。若 afb，则称 b 为 a 的**象**，用 $f(a)$ 表示，而称 a 为 b

的**象源**，也称 a 为自变量，对应的 b 称为函数 f 在 a 处的值。通过 f 和 A 中元素相对应的 B 中的所有元素的集合是 f 的值域 R_f，通常用 $f(A)$表示（参见图 3-1），即

$$f(A)=\{b \mid b\in B，存在\ a\in A，使得\ f(a)=b\}。$$

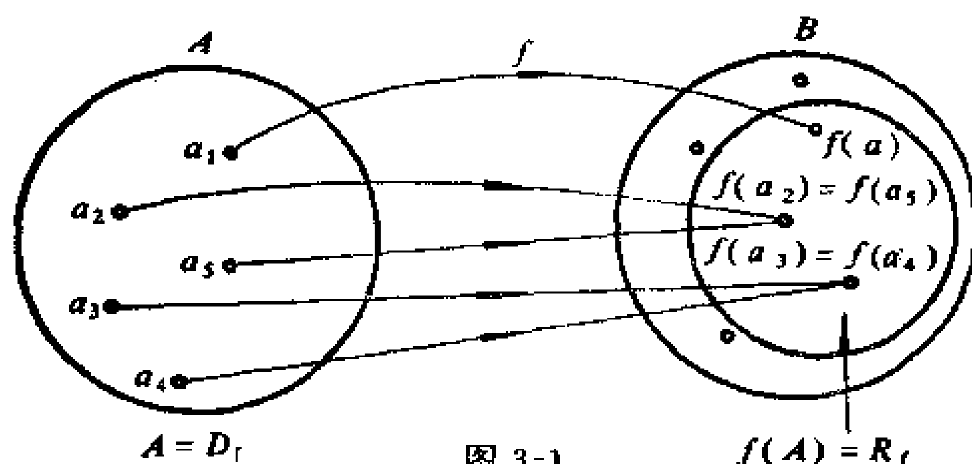


图 3-1

如果 A 本身是一个笛卡尔积 $A=A_1\times A_2\times\cdots\times A_n$，那么 A 中元素在函数 f 作用下的象 $f((a_1,a_2,\cdots,a_n))$ 通常就简写成 $f(a_1,a_2,\cdots,a_n)$.

函数也叫 **"映射"** 或 **"变换"**. 总之是将一个个体变成另一个个体的意思。 如果集合 A 和集合 B 都是通常的数集，不难看出，上面定义的由 A 到 B 的函数就是通常我们所说的函数。因此我们这里所定义的函数是通常函数概念的推广。

图 3-2 给出了一些函数的图示。由图可看出，允许在集合 A 中有多个元素共有一个相同的函数值。例如，对于函数 f_2，$f_2(a_1)=f_2(a_2)=b_3$。也允许集合 B 中有的元素在 A 中没有象源. 例如，对于 f_1 来说，$b_4\in B$ 在 A 中无象源。

例 1 设 $A=\{a,b,c,d\}$，$B=\{2,5,7,9,3\}$，

$$f=\{(a,2),\ (b,7),\ (c,9),\ (d,9)\},$$

则 f 是一由 A 到 B 的函数。$D_f=A, R_f=\{2,7,9\}$。$f(a)=2$，$f(b)=7$，$f(c)=f(d)=9$。

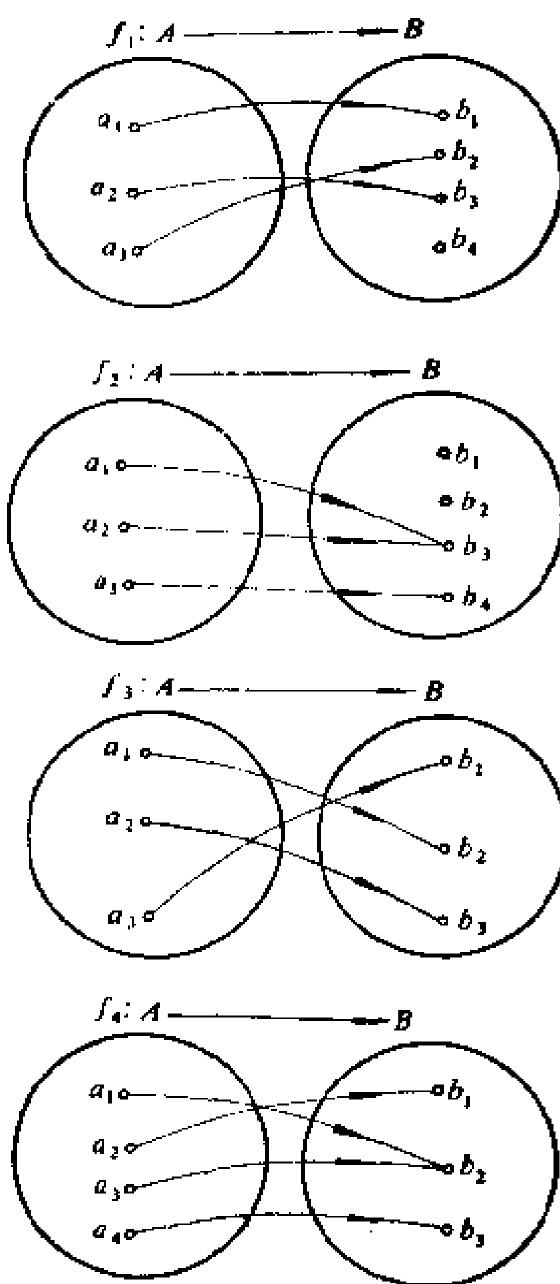


图3-2 函数的示意图

例2 设 $A=I$，$B=N$，$f=\{(i,|2i|+1)\,|\,i\in I\}$ 或 $f(i)=|2i|+1\ (i\in I)$，则 f 是一由整数集 I 到正整数集 N 的函数。其值域是全部正奇数的集合。

例3 设 $A=B=R$，又设 $f=\{(a,a^2)\,|\,a\in R\}$，$g=\{(a^2,a)\,|\,a\in R\}$。

显然，f 是从 R 到 R 的函数，但 g 不是一个函数，因为象的存在性和唯一性条件都不能满足。例如，序偶 $(4,2)$ 和 $(4,-2)$ 都属于 g。又如，$-4\in R$ 在 R 中无象。

定义 3-2 设有函数 $f: A\to B$ 和 $g: C\to D$，如果 $A=C$ 和 $B=D$，并且对所有的 $a\in A$（或 $a\in C$）都有 $f(a)=g(a)$，则称函数 f 和 g 是**相等**的，记为 $f=g$。

定义 3-3 设有函数 $f: A\to B$ 和 $g: \tilde{A}\to B$，如果 $\tilde{A}\subseteq A$，且对于所有的 $a\in\tilde{A}$，有 $g(a)=f(a)$，则称 g 是 f 在 $\tilde{A}$ 上的**限制**，并称 f 是 g 在 A 上的**扩充**。

由定义，显然有 $g=f\cap(\tilde{A}\times B)$。

例4 函数 $g: Z\to N$，定义为 $g(z)=2z+1$，就是例 2 中函数 $f: I\to N$ 在非负实数集上的限制。

例 5　函数 $h: R_0 \to R$，定义为 $h(a)=a^2$（R_0 表示非负实数集），就是例 3 中的函数 $f: R\to R$ 在非负实数集 R_0 上的限制。

函数的限制和扩充是经常见到的概念。要注意的是，一个函数与它的限制或扩充是不相同的函数，它们往往还具有完全不同的性质。

我们知道，$A\times B$ 的每一个子集都是由 A 到 B 的一个关系，但这些子集并不都是由 A 到 B 的函数，其中只有一部分子集可以用来定义由 A 到 B 的函数。我们用 B^A 表示这些函数的集合，亦即

$$B^A=\{f \mid f: A\to B\}.$$

当 A 和 B 都是有限集时，为了确定从 A 到 B 的函数的个数，我们假设 $\# A=m$，$\# B=n$，因为任一函数 f 是由 A 的 m 个元素上的取值所唯一地确定，而对于 A 中的任一元素 a，f 在 a 处的取值都有 n 种可能，因此由 A 到 B 的不同函数共有 $\underbrace{n\cdot n\cdot \cdots \cdot n}_{m}=n^m$ 个，亦即 $\#(B^A)=(\# B)^{\# A}$。

例 6　设 $A=\{a,b\}$，$B=\{0,1\}$，

$$A\times B=\{(a,0),\ (a,1),\ (b,0),\ (b,1)\}.$$

$A\times B$ 有 2^4 个不同的子集，其中只有 2^2 个子集定义由 A 到 B 的函数，它们是：

$$f_1=\{(a,0),\ (b,0)\};\quad f_3=\{(a,1),\ (b,0)\};$$
$$f_2=\{(a,0),\ (b,1)\};\quad f_4=\{(a,1),\ (b,1)\}.$$

下面介绍三种特殊的函数。

定义 3-4　设 f 是一个由 A 到 B 的函数。

(1) 若当 $a_i\neq a_j$ 时，有 $f(a_i)\neq f(a_j)$（也就是当 $f(a_i)=f(a_j)$ 时，有 $a_i=a_j$），则称 f 为由 A 到 B 的**内射**。

(2) 若 $f(A)=B$，则称 f 为由 A 到 B 的**满射**。

(3) 若 f 既是内射又是满射，则称 f 为由 A 到 B 的**双射**。

由定义，所谓内射就是集合 A 中不同的元素在 B 中有不同的

象，或者说 B 中的元素如果有象源，则只有唯一的象源。因此，内射使得集合 A 的元素与 f 的值域 R_f 的元素之间一一对应。所谓满射，即 B 中每一个元素都是 A 中至少一个元素的象。若 f 是双射，则不仅 A 中每一个元素在 B 中有唯一的象，而且 B 中每一个元素在 A 中有唯一的象源，因此 f 必使得集合 A 与集合 B 的元素间一一对应。显然，如果 A 和 B 都是有限集，那么只有当 A 中的元素个数少于或等于 B 中的元素个数，即 $\#A \leqslant \#B$ 时，$f: A \to B$ 才有可能是内射；只有当 $\#A \geqslant \#B$ 时，$f: A \to B$ 才有可能是满射；只有 $\#A = \#B$ 时，$f: A \to B$ 才有可能是双射。

在图 3-2 所给出的函数中，f_1 是内射但不是满射；f_4 是满射但不是内射；f_2 既不是满射也不是内射；f_3 既是满射又是内射，因而是双射。

例 7 函数 $f: Z \to Z$，这里 $f(z) = 2z$，就是一个由非负整数集到自身的内射，但它不是满射。

例 8 函数 $f: I \to Z_5$，这里 $f(i) = \mathrm{res}_5(i)$，是一个由整数集到集 $\{0, 1, 2, 3, 4\}$ 的满射，但不是内射。

例 9 函数 $f: 2^U \to 2^U$，这里 $f(S) = S'$，是一个由 U 的幂集到自身的双射。

现在我们再回过头去看看例 3 中的 $f: R \to R$ 和 f 在非负实数集 R_0 上的限制 h（见例 5），显然，函数 f 既不是内射又不是满射，但 h 是内射。

例 10 设集合 $A = \{a_1, a_2, \cdots, a_n\}$，$B = \{0, 1\}$。对于 A 的任一子集 S，我们将它对应如下的有序 n 元组 $f(S) = (b_1, b_2, \cdots, b_n)$，其中

$$b_i = \begin{cases} 1 & \text{若 } a_i \in S, \\ 0 & \text{若 } a_i \notin S. \end{cases} \quad (i = 1, 2, \cdots, n)$$

显然，f 是一个由 A 的幂集 2^A 到集合 B^n 的函数，而且可以证明 f 是由 2^A 到 B^n 的双射。

首先，对于集合 B^n 中任一有序 n 元组 $(b_1, b_2, \cdots, b_n)$，令

$$S = \{a_i \mid a_i \in A, b_i = 1\},$$

则有 $S \subseteq A$ 且 $f(S) = (b_1, b_2, \cdots, b_n)$。这说明 f 是由 2^A 到 B^n 的满射。

其次，对于 B^n 中任一有序 n 元组 $(b_1, b_2, \cdots, b_n)$，按上述方法已知它有象源 S。现假设它还有一象源 $\tilde{S} \in 2^A$，即 $f(\tilde{S}) = (b_1, b_2, \cdots, b_n)$，则

$$a_i \in S \Leftrightarrow b_i = 1 \Leftrightarrow a_i \in \tilde{S}$$[注]。

这就意味着 $S = \tilde{S}$，因此 B^n 中任一元素只有一个象源。于是证明了 f 是由 2^A 到 B^n 的双射。

因为 f 是由 2^A 到 B^n 的双射，所以集合 2^A 中元素个数必等于集合 B^n 中元素个数，而 $\#(B^n) = (\#B)^n = 2^n$，故 $\#(2^A) = 2^n$。这就再一次地证明了 n 个元素的集合一共有 2^n 个子集。

事实上，上例中集合 B^n 中的所有有序 n 元组就是 §1.3 中用来表示集合 A 的各子集的二进制形式的下标。正因为 2^A 与 B^n 的元素是一一对应的，因此我们可用 §1.3 中所介绍的表示方法来方便地表示集合 A 的各子集。

集合 A 上的恒等关系 $I_A = \{(a, a) \mid a \in A\}$ 显然是一个由 A 到 A 的双射，对于每一个元素 $a \in A$，其象就是元素 a 自身。我们称 I_A 为集合 A 上的恒等函数。

§3.2 函数的复合

定义 3-5 设有函数 $f: A \to B$，$g: B \to C$，则 f 和 g 的**复合函数**是一个由 A 到 C 的函数，记为 $g \circ f$（或简记成 gf）。对于任一 $a \in A$，有 $(g \circ f)(a) = g(f(a))$。即如果 $b \in B$ 是 $a \in A$ 在 f 作用下的象，且 $c \in C$ 是 b 在 g 作用下的象，那么 c 就是 a 在 gf 作用下的象。

[注] "$\Leftrightarrow$"表示该记号两端的条件是等价的，以后相同。

定义 3-5 是定义 2-5 对于函数这一特殊关系的另一种叙述形式。实际上，这里定义的复合函数 $g\cdot f$：$A\to C$ 也就是定义 2-5 中所说的由 A 到 C 的复合关系 $f\cdot g$。需注意的是，当复合关系是一个复合函数时，在其表示记号中颠倒了 f 和 g 的位置而写成 $g\cdot f$，为的是与通常意义下复合函数的表示方法一致。

图 3-3 给出了复合函数 $g\cdot f$ 的图示。

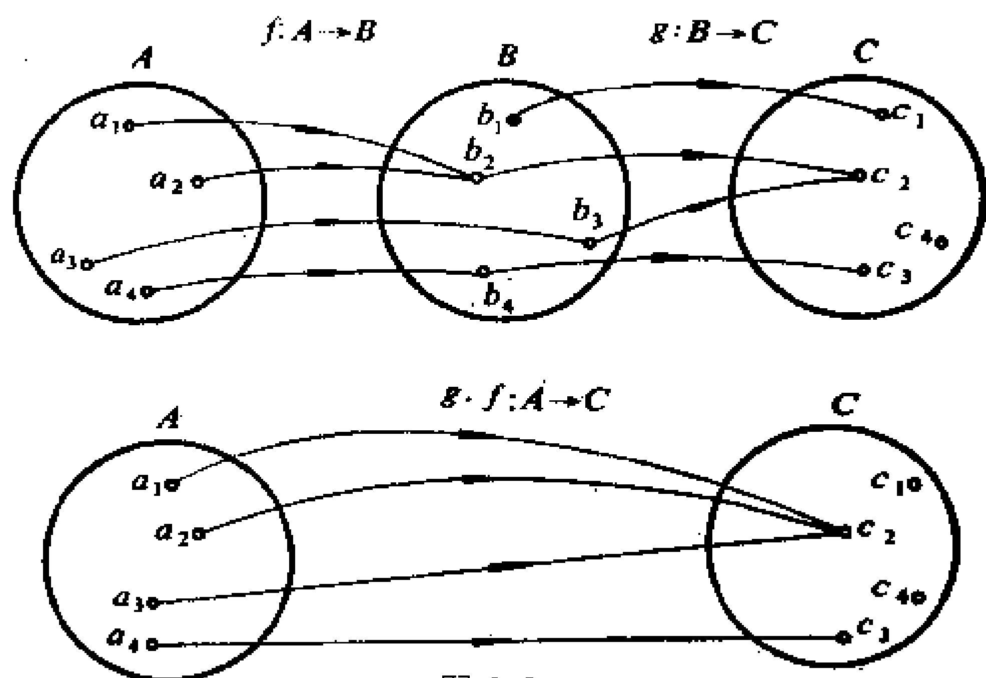


图 3-3

在上述复合函数的定义中，要求 f 的值域包与 g 的定义域相等。实际上，对此条件可以放宽，只要求 f 的值域 $R_f\subseteq D_g$，即若有函数 f：$A\to B$，g：$C\to D$，且 $R_f\subseteq C$，则同样可以定义一个由 A 到 D 的复合函数 $g\cdot f$。但若 $R_f\nsubseteq C$，则 $g\cdot f$ 就没有意义了。因此在定义 3-5 的条件下，虽然 $g\cdot f$ 有意义，但 $f\cdot g$ 不一定有意义。即使 $g\cdot f$ 与 $f\cdot g$ 都有意义，二者也不一定相等。

例 1 设 $A=\{1,2,3\}$，$B=\{a,b\}$，$C=\{e,f\}$，

f：$A\to B$，$f=\{(1,a),\ (2,a),\ (3,b)\}$，

g：$B\to C$，$g=\{(a,e),\ (b,e)\}$，

则 $$gf=\{(1,e),\ (2,e),\ (3,e)\}$$
是一由A到C的函数。

例 2 设有函数$f: 2^A\to Z$,其中A是一有限集合,且$f(S)=\#S$。函数$g: Z\to R$, $g(Z)=\frac{Z-5}{2}$,则复合函数$gf: 2^A\to R$, 对于任意的$S\subseteq A$, 有

$$(gf)(S)=g(f(S))=g(\#S)=\frac{\#S-5}{2}.$$

例 3 设$A=\{1,2,3\}$, 函数

$$f: A\to A,\ f=\{(1,2),\ (2,3),\ (3,1)\},$$
$$g: A\to A,\ g=\{(1,2),\ (2,1),\ (3,3)\},$$

则复合函数

$$gf=\{(1,1),\ (2,3),\ (3,2)\},$$
$$fg=\{(1,3),\ (2,2),\ (3,1)\}\neq gf.$$
$$ff=\{(1,3),\ (2,1),\ (3,2)\},$$
$$gg=\{(1,1),\ (2,2),\ (3,3)\}.$$

因为函数的复合是关系复合的一种特殊情形,因此关系复合中成立的性质,对于函数复合也是成立的。例如,对于任一函数$f: A\to B$, 有$fI_A=I_Bf=f$。又如,设有三个函数$f: A\to B$, $g: B\to C$, $h: C\to D$, 根据定义 3-5,这些函数可以构成复合函数$gf: A\to C$, $hg: B\to D$, 进而可以构成复合函数$h(gf)$和$(hg)f$, 二者都是由A到D的函数。因为关系的复合是可结合的,当然函数的复合也是可结合的,因此有下面的定理。

定理 3-1 设有函数$f: A\to B$, $g: B\to C$, $h: C\to D$, 则有

$$h(gf)=(hg)f.$$

现根据复合函数的定义,给出该定理的证明。

证明 因为对于任意的$a\in A$, 有

$$[h(gf)](a)=h[(gf)(a)]=h(g(f(a)))$$
$$=(hg)(f(a))=[(hg)f](a),$$

所以，$h(gf)=(hg)f$。证完。

由于函数复合的可结合性，因此通常去掉括号而写成 hgf。一般地，设有 n 个函数 $f_1: A_1\to A_2, f_2: A_2\to A_3, \cdots, f_n: A_n\to A_{n+1}$。则不加括号的表达式 $f_nf_{n-1}\cdots f_1$ 唯一地表示一个由 A_1 到 A_{n+1} 的函数。

特别，当 $A_1=A_2=\cdots=A_{n+1}=A$ 且 $f_1=f_2=\cdots=f_n=f$ 时（即当所有的 f_i 都是由集合 A 到 A 的同一函数时），复合函数 $f_nf_{n-1}\cdots f_1$（是一个由 A 到 A 的函数）可表示为 f^n。

例4 设有函数 $f: I\to I$，给定为 $f(i)=2i+1$，试求复合函数 f^3。

解 由定义 3-5，复合函数 f^3 也是由 I 到 I 的函数。对于任意的 $i\in I$，

$$
\begin{aligned}
f^3(i) &= f(f^2(i)) = 2f^2(i)+1 = 2f(f(i))+1 \\
&= 2(2f(i)+1)+1 = 4f(i)+3 \\
&= 4(2i+1)+3 = 8i+7.
\end{aligned}
$$

定义 3-6 设 f 是一个由 A 到 A 的函数，且 $f^2=f$，则称 f 是**幂等函数**。

例 5 函数 $f: 2^N\to 2^N$，给定为 $f(S)=\{n|n\in S\cap P\}$，则 f 是一个幂等函数。因为由 f 的定义，对于任一 $S\in 2^N$，$f(S)$ 为 S 中所有素数的集合，记为 S_P ($S_P\subseteq N$)。而 $f^2(S)=f(f(S))=f(S_P)=S_P$。所以 $f^2=f$。

如果 f 是幂等的，则对于所有的正整数 $n\geqslant 1$，都有 $f^n=f$。

定理 3-2 设有函数 $f: A\to B$ 和 $g: B\to C$。

(1) 如果 f 和 g 都是内射，则 gf 也是内射；

(2) 如果 f 和 g 都是满射，则 gf 也是满射；

(3) 如果 f 和 g 都是双射，则 gf 也是双射。

证明 (1) 设 $a_i, a_j\in A$ 且 $a_i\neq a_j$，由于 f 是内射，因此 $f(a_i)\neq f(a_j)$；由于 g 也是内射，故又有 $g(f(a_i))\neq g(f(a_j))$，此即由 $a_i\neq a_j$，可得 $(gf)(a_i)\neq(gf)(a_j)$，故 gf 是内射。

(2) 设任一元素 $c\in C$，由于 g 是满射，因此必存在某一 $b\in B$，

使得 $g(b)=c$。又由于 f 也是满射，因而必存在某一 $a\in A$，使得 $f(a)=b$，于是有 $(gf)(a)=g(f(a))=g(b)=c$，即 $c\in(gf)(A)$。由 c 的任意性，故 gf 是满射。

(3) 由于 f 和 g 都是双射，因此它们既是内射又是满射，由 (1) 和 (2) 可知 gf 是双射。由此定理得证。

例 6 设 I^- 是负整数的集合，定义 f 和 g 是如下的双射：

$$f: I^- \to N,\ f(x) = -x,$$

$$g: N \to Z,\ g(x) = x-1.$$

因而复合函数 $gf: I^- \to Z$ 也是双射，且 $gf(x) = -x-1$。

定理 3-2 的逆定理不成立。但有下面"部分可逆"的结论。我们只给出 (1) 的证明，其余两条的证明留给读者作为练习。

定理 3-3 设有函数 $f: A\to B$ 和 $g: B\to C$。

(1) 如果 gf 是内射，则 f 是内射；

(2) 如果 gf 是满射，则 g 是满射；

(3) 如果 gf 是双射，则 f 是内射而 g 是满射。

证明 (1)假设 f 不是内射，则必存在两个元素 $a_i, a_j\in A$，$a_i\neq a_j$，使得 $f(a_i)=f(a_j)$。令 $f(a_i)=f(a_j)=b$，且令 $g(b)=c$。则由复合函数的定义有

$$(gf)(a_i)=g(f(a_i))=g(b)=c,$$

$$(gf)(a_j)=g(f(a_j))=g(b)=c,$$

此即 $(gf)(a_i)=(gf)(a_j)$ 与 gf 是内射矛盾。故 f 是内射。证完。

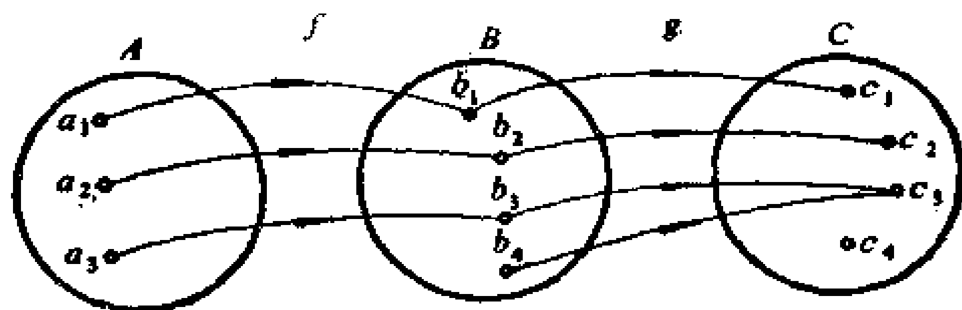


图 3-4

然而当 gf 是内射时，g 可以不是内射。如图3-4所示就是一例，复合函数 gf 是内射，但 g 不是内射。在那里 $g(b_3)=g(b_4)=c_3$，但 $b_3 \neq b_4$。

§3.3 逆函数

在第二章我们曾把由集 A 到集 B 的关系 ρ 的逆关系 $\tilde{\rho}$ 定义为由 B 到 A 的关系，当且仅当 $(a,b)\in\rho$ 时，有 $(b,a)\in\tilde{\rho}$。也就是简单地交换 ρ 的所有序偶中的元素，就可得到逆关系 $\tilde{\rho}$ 的各个序偶。对于函数来说，情况就不这么简单。如果 f 是一个从 A 到 B 的函数，因为 f 也是一个关系，因此可以按上述方法得到 f 的逆关系 $\tilde{f}$，但 $\tilde{f}$ 可能不是一个函数。例如，如果 f 不是一个满射，则 $\tilde{f}$ 的定义域就只能是 B 的一个真子集而不能是 B。又如果 f 不是一个内射，例如有 $(a_1,b)\in f$，$(a_2,b)\in f$，则有 $(b,a_1)\in\tilde{f}$，$(b,a_2)\in\tilde{f}$，因而 $\tilde{f}$ 不满足象的唯一性条件。

例1 设 $A=\{0,1\}$，$B=\{p,q,r,s\}$，

$f: A\to B$ 由 $f=\{(0,p),(1,r)\}$ 给出。

则
$$\tilde{f}=\{(p,0),\ (r,1)\},$$
显然，$\tilde{f}$ 不是由 B 到 A 的函数。

例2 设 $f: R\to R$ 由 $f=\{(a,a^2)\,|\,a\in R\}$ 给出，

则
$$\tilde{f}=\{(a^2,a)\,|\,a\in R\}$$
不是从 R 到 R 的函数。

例3 设 $A=\{1,2,3,4\}$，$B=\{p,q,r\}$，

$f: A\to B$ 由 $f=\{(1,p),(2,q),(3,q)(4,r)\}$

给出，则
$$\tilde{f}=\{(p,1),(q,2),(q,3),(r,4)\}$$
显然也不是一个函数。

如果 f 是一个由 A 到 B 的双射，则对于 B 中每一个元素 b，

一定有一个而且只有一个 $a\in A$，使得 $f(a)=b$。如果把这唯一对应的 a 看作是 b 在某个映射下的象，就可得到一个由 B 到 A 的函数。我们称它为 f 的逆函数。

定义 3-7 设有函数 $f: A\to B$ 是一个双射，定义函数 $g: B\to A$，使得对于每一个元素 $b\in B$，$g(b)=a$，其中 a 是使得 $f(a)=b$ 的 A 中的元素，则称 g 为 f 的**逆函数**，记作 f^{-1}。若函数 f 存在逆函数 f^{-1}，则称 f 是**可逆的**。

注意，仅当 f 是双射函数时，才定义 f 的逆函数 f^{-1}，而且 f^{-1} 就是 f 的逆关系 $\tilde{f}$。

定理 3-4 设函数 $f: A\to B$ 是双射，则逆函数 $f^{-1}: B\to A$ 也是一个双射。

证明 对于任一元素 $a\in A$，由函数 f 的定义，在 B 中必有一元素 b，使得 $f(a)=b$，于是由逆函数 f^{-1} 的定义，$f^{-1}(b)=a$，即 $a\in f^{-1}(B)$，由 a 的任意性，可知 f^{-1} 是一个满射。又设 $b_1, b_2\in B$，且 $b_1\neq b_2$，由双射函数 f 的定义，在 A 中必有两个元素 $a_1\neq a_2$，使得 $f(a_1)=b_1, f(a_2)=b_2$。于是 $f^{-1}(b_1)=a_1, f^{-1}(b_2)=a_2$，并且 $f^{-1}(b_1)\neq f^{-1}(b_2)$，这就是说 f^{-1} 是一个内射。

因为 f^{-1} 既是一个满射又是一个内射，所以 f^{-1} 是一个双射。定理得证。

既然 f^{-1} 也是一个双射，那么 f^{-1} 也应有逆函数。

定理 3-5 设函数 $f: A\to B$ 是一个双射，则 $(f^{-1})^{-1}=f$。

证明 由定理 3-4 f^{-1} 是一个由 B 到 A 的双射。因此 $(f^{-1})^{-1}$ 与 f 一样也是一个由 A 到 B 的函数。对于任一元素 $a\in A$，设 $f(a)=b$，则 $f^{-1}(b)=a$，因而 $(f^{-1})^{-1}(a)=b$，于是 $f(a)=(f^{-1})^{-1}(a)$，由 a 的任意性，即知 $(f^{-1})^{-1}=f$。证完。

定理3-5说明 f 和 f^{-1} 互为逆函数，它们之间还有以下的关系。

定理 3-6 如果函数 $f: A\to B$ 是可逆的，则有

$$f^{-1}f=I_A,\quad ff^{-1}=I_B.$$

证明 由复合函数的定义，$f^{-1}f$ 是一由 A 到 A 的函数。对于任一元素 $a\in A$，设 $f(a)=b$，则 $f^{-1}(b)=a$，于是 $(f^{-1}f)(a)=f^{-1}(b)=a$，由 a 的任意性，即得 $f^{-1}f=I_A$。类似地可以证明 $ff^{-1}=I_B$。证完。

值得注意的是，虽然 $f^{-1}f$ 与 ff^{-1} 都是恒等函数，但有不同的定义域，所以我们不能简单地写 $ff^{-1}=I$。只要 $A\neq B$，总有 $ff^{-1}\neq f^{-1}f$。

定理 3-7 设有函数 $f: A\to B$ 和 $g: B\to A$，当且仅当 $gf=I_A$，$fg=I_B$ 时，有 $g=f^{-1}$。

证明 必要性直接由定理3-6可得。下面证明充分性。

因为 $fg=I_B$ 是一满射，故由定理 3-3，f 是一满射；因为 $gf=I_A$ 是一内射，故由定理 3-3，f 是一内射。因而 f 是一双射，有逆函数 f^{-1}。

由于 $$f^{-1}(fg)=f^{-1}I_B=f^{-1},\quad (f^{-1}f)g=I_Ag=g.$$

故有 $$g=f^{-1}.$$ 证完

定理 3-8 设有函数 $f: A\to B$ 和 $g: B\to C$，且 f 和 g 都是可逆的。则

$$(gf)^{-1}=f^{-1}\cdot g^{-1}.$$

证明 因为 f 和 g 都可逆，所以存在有逆函数 $f^{-1}: B\to A$，$g^{-1}: C\to B$，因而有复合函数 $f^{-1}g^{-1}: C\to A$。又因为 f 和 g 都是双射，由定理 3-2，gf 也是双射，因此有逆函数 $(gf)^{-1}: C\to A$。于是 $(gf)^{-1}$ 与 $f^{-1}g^{-1}$ 都是由 C 到 A 的函数。

对于任一元素 $c\in C$，设 $g^{-1}(c)=b$，$f^{-1}(b)=a$，

则 $$(f^{-1}g^{-1})(c)=f^{-1}(b)=a.$$

而 $$(gf)(a)=g(f(a))=g(b)=c,\ \text{所以}\ (gf)^{-1}(c)=a.$$

因此 $$(f^{-1}g^{-1})(c)=(gf)^{-1}(c).$$

由 c 的任意性，故有 $(gf)^{-1}=f^{-1}g^{-1}$。证完。

此定理说明，复合函数的逆函数能够用相反次序的逆函数的

复合来表示。

§3.4 置　　换

这一节介绍一种更为特殊的函数，即从有限集 A 到 A 自身的双射函数。

定义 3-8 设 $A=\{a_1,a_2,\cdots,a_n\}$ 是一个有限集合，从 A 到 A 的双射函数称为集合 A 上的**置换**。而整数 n 称为**置换的阶**。

一个 n 阶置换 $P: A\to A$ 常表示成如下形式：

$$P=\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ P(a_1) & P(a_2) & \cdots & P(a_n) \end{pmatrix}.$$

这里 n 个列的次序当然是任意的，由于 P 是双射，因此 $P(a_1)$，$P(a_2)$，$\cdots$，$P(a_n)$ 各不相同，然而所有的 $P(a_i)$ 都是 A 中的元素，因此 $P(a_1)$，$P(a_2)$，$\cdots$，$P(a_n)$ 必为 a_1，a_2，$\cdots$，a_n 的一个排列。由于 a_1，a_2，$\cdots$，a_n 上排列的总数等于 $n!$，因此集合 A 上不同的 n 阶置换的数目是 $n!$ 个。

例如，设 $A=\{1,2,3\}$，因为 $n=3$，所以集合 A 上应有 $3!=6$ 个不同的三阶置换，它们是：

$$P_1=\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},\ P_2=\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},\ P_3=\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$$P_4=\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},\ P_5=\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},\ P_6=\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

集合 A 上的恒等函数 $I_A=\{(a,a)\mid a\in A\}$ 是集合 A 上形为

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$$

的一个置换，称它为 A 上的**恒等置换**。上例中的 P_1 就是 $A=\{a,b,c\}$ 上的恒等置换。

因为双射函数是可逆的，所以集合 A 上的任何置换 $P: A\to A$

都有逆函数 P^{-1}: $A \to A$，它也是由 A 到 A 的双射，因此也是 A 上的置换。我们称 P^{-1} 为 P 的逆置换。若

$$P = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ P(a_1) & P(a_2) & \cdots & P(a_n) \end{pmatrix},$$

则

$$P^{-1} = \begin{pmatrix} P(a_1) & P(a_2) & \cdots & P(a_n) \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}.$$

上例中的 $P_1^{-1} = P_1$，$P_2^{-1} = P_2$，$P_3^{-1} = P_3$，$P_4^{-1} = P_5$，$P_5^{-1} = P_4$，$P_6^{-1} = P_6$。

设 P_1: $A \to A$，P_2: $A \to A$ 是 A 上任意的两个置换，则置换的复合 $P_1 \cdot P_2$: $A \to A$ 也必定是 A 上的一个置换。这就是说，置换在复合运算下是封闭的。有关置换的其它一些性质，我们将在第五章再作介绍。

§3.5 集合的特征函数

在这一节里我们讨论从全集合 U 到集合 $\{0, 1\}$ 的函数，即 f: $U \to \{0, 1\}$。我们知道，这样的函数不止一个。如果 U 是有限集，若 $|U| = n$，则有 2^n 个这样的函数；若 U 是无限集，则这样的函数有无穷多个。

因为 f 是由 U 到 $\{0, 1\}$ 的函数，因此 U 中每一元素在集合 $\{0, 1\}$ 中都有象，其象不是 1 就是 0。若令 U 的子集 $A = \{u | u \in U, f(u) = 1\}$，则每一个函数 f 必对应着 U 的这样一个子集。反之，对于 U 的每一个子集 A，我们定义一函数 $f: U \to \{0, 1\}$，使得当 $u \in A$ 时，$f(u) = 1$；当 $u \notin A$ 时，$f(u) = 0$。则 U 的每一子集 A 必对应着一个由 U 到 $\{0, 1\}$ 的函数。因此集合 $\{0, 1\}^U$ 与全集 U 的幂集 2^U 的元素之间有着一一对应关系（即存在着由 $\{0, 1\}^U$ 到 2^U 的双射）。我们把每一个由 U 到 $\{0, 1\}$ 的函数称为相对应的子集的特征函数。

定义 3-9 全集合U的子集A的**特征函数**定义为 $e_A: U \to \{0, 1\}$，这里

$$e_A(u)=\begin{cases}1 & 当 u\in A,\\ 0 & 当 u\notin A.\end{cases}$$

特征函数有下述一些性质：

1. 设A和B是全集U的两个子集，于是

(1) 当且仅当对所有的$u\in U$，$e_A(u)=0$，则$A=\phi$；

(2) 当且仅当对所有的$u\in U$，$e_A(u)=1$，则$A=U$；

(3) 当且仅当对所有的$u\in U$，$e_A(u)\leqslant e_B(u)$，则$A\subseteq B$；

(4) 当且仅当对所有的$u\in U$，$e_A(u)=e_B(u)$，则$A=B$。

2. 设A和B是全集U的两个子集，则对于所有的$u\in U$，有

(1) $e_{A'}(u)=1-e_A(u)$；

(2) $e_{A\cup B}(u)=e_A(u)+e_B(u)-e_A(u)\cdot e_B(u)$；

(3) $e_{A\cap B}(u)=e_A(u)\cdot e_B(u)$。

注意，由于特征函数的值是 0 或 1，因此用于特征函数间的关系符号和运算符号$\leqslant$、$=$、$+$、$-$和$\cdot$都是表示通常的数的关系和算术运算。

上述性质由特征函数的定义都容易得到证明。下面仅以 1(4) 和 2(3) 为例给出其证明。

证明 1(4) 假设对所有的$u\in U$，$e_A(u)=e_B(u)$ 成立。并设任一元素$u\in A$，则$e_A(u)=1$。因为$e_A(u)=e_B(u)$，所以$e_B(u)=1$。由特征函数e_B的定义，有$u\in B$，因而有$A\subseteq B$。类似地可证明$B\subseteq A$，故$A=B$。

反之，设$A=B$，对于任一元素$u\in U$，若$u\in A$，则由$A=B$，有$u\in B$，因此$e_A(u)=e_B(u)=1$；若$u\notin A$，则由$A=B$，有$u\notin B$，因此$e_A(u)=e_B(u)=0$。故对任意的元素$u\in U$，有$e_A(u)=e_B(u)$。证完。

2(3) 对任意的$u\in U$，若$u\in A\cap B$，则$u\in A$且$u\in B$，因而

有 $e_{A\cap B}(u)=e_A(u)=e_B(u)=1$，所以 $e_{A\cap B}(u)=e_A(u)\cdot e_B(u)=1$；若 $u\notin A\cap B$，则 $u\notin A$ 或 $u\notin B$，而因有 $e_{A\cap B}(u)=0$，且有 $e_A(u)=0$ 或 $e_B(u)=0$，所以 $e_{A\cap B}(u)=e_A(u)\cdot e_B(u)=0$。故性质 2(3) 得证。

特征函数的上述性质可用来证明各种集合恒等式。

例 1 $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$

证明 由特征函数的性质 2(3)、(2)，对于所有的 $u\in U$，有

$$\begin{aligned}
&e_{A\cap(B\cup C)}(u)\\
&=e_A(u)\cdot e_{B\cup C}(u)\\
&=e_A(u)\cdot(e_B(u)+e_C(u)-e_B(u)\cdot e_C(u))\\
&=e_A(u)\cdot e_B(u)+e_A(u)\cdot e_C(u)-e_A(u)\cdot e_B(u)\cdot e_A(u)\cdot e_C(u)\\
&=e_{A\cap B}(u)+e_{A\cap C}(u)-e_{A\cap B}(u)\cdot e_{A\cap C}(u)\\
&=e_{(A\cap B)\cup(A\cap C)}(u).
\end{aligned}$$

所以，由性质 1(4) 有 $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$。证完。

例 2 $(A')'=A$

证明 由性质 2(1)，对所有的 $u\in U$，有

$$\begin{aligned}
e_{(A')'}(u)&=1-e_{A'}(u)\\
&=1-(1-e_A(u))\\
&=e_A(u).
\end{aligned}$$

因此有 $(A')'=A$。证完。

设有函数 $f: A\to B$，定义 A 上的关系 ρ_f：当且仅当 $f(a_i)=f(a_j)$ 时，有 $a_i\rho_f a_j$。容易验证，ρ_f 是 A 上的一个等价关系（称 ρ_f 为 f 的等价核），因此它可以导致 A 上的一个等价分划 $\pi_{\rho_f}^A=\{[a]_{\rho_f}|a\in A\}$，其中 $[a]_{\rho_f}$ 是等价类。由于同一等价类中的元素都以 B 中同一元素为象，因此每一等价类对应着 f 的值域中的一个元素。反之，f 的值域中的每一个元素在 A 中至少有一个象源，因而该元素必与其象源所在的等价类对应。于是存在一个由分划 $\pi_{\rho_f}^A$ 到 f 的值域的双射。若 f 的值域为有限，即若 $R_f=\{b_1,b_2,\cdots,b_k\}\subseteq B$，则 $\pi_{\rho_f}^A=\{A_1,A_2,\cdots,A_k\}$，其中 $A_i=\{a|a\in A, f(a)=b_i\}(i=$

$1,2,\cdots,k$)。因为对于任一个 $a\in A$，必存在且只存在一个 $i(1\leqslant i\leqslant k)$，使得 $a\in A_i$，对于 $j\neq i$，$a\notin A_j$。所以 $e_{A_1}(a)$，$e_{A_2}(a),\cdots$，$e_{A_k}(a)$ 中只有 $e_{A_i}(a)=1$，其它 $e_{A_j}(a)=0(j\neq i)$。于是我们可将 $f(a)=b$ 写成如下形式：

$$f(a)=b_1e_{A_1}(a)+b_2e_{A_2}(a)+\cdots+b_ie_{A_i}(a)+\cdots+b_ke_{A_k}(a),$$

即对于所有的 $a\in A$，有

$$f(a)=\sum_{i=1}^{k}b_ie_{A_i}(a).$$

这说明特征函数可以用来表示具有有限值域的函数。

例 3 函数 $f:I\to Z_m$ 定义为 $f(i)=\text{res}_m(i)$，显然 f 是值域 $R_f=Z_m$ 的一个满射。

令 $\quad C_j=\{i\mid i\in I,\ \ i\equiv j(\text{mod}\, m)\}(j=0,1,2,\cdots,m-1)$，

则 $\quad \pi^I_{D_f}=\{C_0,C_1,C_2,\cdots,C_{m-1}\}$ 是 I 的一个分划，

因此 $\quad f(i)=0e_{C_0}(i)+1e_{C_1}(i)+2e_{C_2}(i)+\cdots+(m-1)e_{C_{m-1}}(i)$，

即

$$f(i)=\sum_{j=0}^{m-1}je_{C_j}(i).$$

在第一章我们曾介绍过集合的成员表。设 A,B 是全集合 U 的子集，那么根据补、并、交的定义，可作出 A'、$A\cap B$ 和 $A\cup B$ 的成员表（参见表 3-1）。

表 3-1

A	B	A'	$A\cap B$	$A\cup B$
0	0	1	0	0
0	1	1	0	1
1	0	0	0	1
1	1	0	1	1

表 3-2

e_A	e_B	$e_{A'}$	$e_{A\cap B}$	$e_{A\cup B}$
0	0	1	0	0
0	1	1	0	1
1	0	0	0	1
1	1	0	1	1

仿照作成员表的方法，由 $e_A(u)$ 和 $e_B(u)$ 的值的所有可能的组合，根据特征函数的性质 2 所给出的公式，把计算出的 $e_{A'}(u)$、

$e_{A\cap B}(u)$ 和 $e_{A\cup B}(u)$ 的相应值也列成表，可得表 3-2。

比较表3-1和表3-2可以看出，表3-1中集合 S 所标记的列在表 3-2 中由该集合的特征函数 e_S 所标记，两者取值的情形完全一样。这是由于成员表和特征函数两定义中的 0 与 1 所代表的意义完全相同。因此一般地，如果 S 是一个由 A_1, A_2, …, A_r 产生的集合，则根据 $e_{A_1}(u), e_{A_2}(u), \cdots, e_{A_r}(u)$ 的值的所有可能的组合而计算出的相应 $e_S(u)$ 的值的表也必然与 S 的成员表完全一样。由此可见，成员表是表达集合的特征函数的一个方法。

§3.6 数学归纳法及其应用

自然数集 N 和它的许多性质早已为人们所熟知。在这一节里，我们不叙述以它的基本性质为特征的公理[注]，只叙述它的某些基本性质，目的在介绍数学归纳法的证明方法和定义方法，以备以后引用。

我们知道，"小于或等于"关系是自然数集 N 上的全序关系，特别对于任意两个自然数 n_1 和 n_2，必有 $n_1 \leqslant n_2$ 或 $n_2 \leqslant n_1$。这一全序关系使得自然数集 N 依照普通数的大小顺序可将其元素排成一个序列：

$$1, 2, 3, 4, 5, \cdots$$

这性质有时称为**自然数的有序性**。

自然数集 N 是无限集，即它的元素个数不是有限数。也就是说，N 里面的数如果依大小的顺序排，那么在任意一个数的后面还有数。

自然数的另一基本性质是**自然数的最小性**。

定理 3-9 在自然数集 N 的任一非空子集 S 中，必定有一个

[注] И. В. 勃罗斯库列亚柯夫著，吴品三译，《数与多项式》(第三章)，高等教育出版社 (1956 年 6 月)。

最小数，也就是说在集 S 中有不大于其他任意数的数。

证明 因为 S 非空，所以可以在 S 中取一数 n，令 S 中所有不大于 n 的数形成的非空集合（至少包含 n）为 T，则显然有 $T\subseteq S$。但从 1 到 n 只有 n 个自然数，因此 T 中所含的数最多只有 n 个，由自然数的有序性可知，T 中必有一最小数，这最小数就是 S 的最小数。证完。

在第二章我们曾说自然数集 N 上的"$\leqslant$"关系是 N 上的良序，其根据也就是自然数的最小性这一性质。由这一性质，我们又可推得下面的重要定理。

定理 3-10 设 S 是由自然数组成的集合，如果 $1\in S$，并且当 $n\in S$ 时，也有 $n+1\in S$，那么 S 含有所有的自然数。

证明 设 E 是 N 中所有不属于 S 的数组成的集合（即 $E=N-S$），如果 E 非空，则由定理 3-9 知，E 中必有一个最小数 a。因为 $a\notin S$，所以 $a\neq 1$，因此 $a-1$ 是自然数，且 $a-1\in S$，于是由假设，有 $a\in S$。这与 $a\notin S$ 矛盾，因此 E 是空集，故 $S=N$。证完。

于是，为了要证明一个命题对于所有的自然数 n 都是真的，我们只要证明两件事：

(1) 当 $n=1$ 时，命题是真的；

(2) 若当 $n=k$ 时这个命题是真的，则当 $n=k+1$ 时这个命题也是真的。

这就是通常的数学归纳法。此外，数学归纳法还有下面的另一种形式。

为了要证明一个命题对于所有的自然数 n 都是真的，我们只要证明两点：

(1) 当 $n=1$ 时，命题是真的；

(2) 若当 $n=1,2,\cdots,k$ 时这个命题是真的，则当 $n=k+1$ 时这个命题也是真的。

这种形式在应用上有时比上面的方便。

定理3-10是数学归纳法原理的基础。下面给出关于数学归纳法证明的合理性定理。

定理 3-11 设 $P(n)$ 是一个与自然数 n 有关的命题，如果对于自然数 1，这个命题为真，而且当对于自然数 k 这个命题为真时，对于 $k+1$ 这个命题也为真，那么命题 $P(n)$ 对于所有的自然数都为真。

证明 令 $S=\{n|n\in N, P(n)\text{为真}\}$，即 S 是使命题 $P(n)$ 为真的所有自然数 n 的集合。如果命题 $P(1)$ 为真，则 $1\in S$。又若 $k\in S$，则命题 $P(k)$ 为真，由假设有 $P(k+1)$ 也为真，因此 $k+1\in S$。这就是说，由 $k\in S$ 可推得 $k+1\in S$。根据定理 3-10，$S=N$，即对于所有的自然数 n，$P(n)$ 都为真。证完。

定理 3-12 设 $P(n)$ 是一个与自然数 n 有关的命题，如果对于自然数 1，这个命题为真，而且当对于自然数 $1, 2, \cdots, k$ 这个命题都为真时，对于 $k+1$ 这个命题也为真，那么命题 $P(n)$ 对于所有的自然数都为真。

证明 令 $J=\{n|n\in N, P(n)\text{为假}\}$，即 J 是使命题 $P(n)$ 为假的所有自然数的集合。若 $J\neq\phi$，则由定理 3-9，J 中有一最小数，设为 j。如果命题 $P(1)$ 为真，则 $1\notin J$，所以 $j>1$，由 j 的最小性可知，当 $n=1, 2, \cdots, j-1$ 时，命题 $P(n)$ 为真（其中 $j-1\geqslant 1$），因而又有命题 $P(j)$ 为真，即 $j\notin J$。这与 j 是 J 中最小数矛盾，因此 $J=\phi$，即对所有的自然数 n，$P(n)$ 都为真。证完。

在应用数学归纳法时，不一定要以 $n=1$ 为基础，我们可以以任何自然数 $n=n_0$ 为基础，在这种情况下，命题对于所有自然数 $n\geqslant n_0$ 成立。

以下给出几个例子，说明数学归纳法的应用。

例 1 试证明对于所有的正整数 $n, n<2^n$。

证明〈归纳基础〉当 $n=1$ 时，有 $1<2^1$。结论成立。

〈归纳步骤〉假设对任一 $k\in N$，有 $k<2^k$，

则 $$k+1<2^k+1<2^k+2^k=2^{k+1},$$

即 $$k+1<2^{k+1}.$$

根据数学归纳法原理，对于所有的 $n\in N$，有 $n<2^n$ 成立。

例 2 试证明对于所有的正整数 $n\geqslant 4$，有 $2^n<n!$。

证明 显然对于 $n=1,2,3$，结论均不成立，我们也不需要它们成立。

〈归纳基础〉 当 $n=4$ 时，$2^4=16$，$4!=24$，因此 $2^4<4!$，结论成立。

〈归纳步骤〉 假设对 N 中任一正整数 $k\geqslant 4$，$2^k<k!$

则 $$2\cdot 2^k<2(k!)<(k+1)\cdot k!=(k+1)!,$$

即 $$2^{k+1}<(k+1)!.$$

所以，对于所有的正整数 $n\geqslant 4$，有 $2^n<n!$ 成立。

例 3 试证明对于所有的正整数 n，有

$$(A_1\cup A_2\cup\cdots\cup A_n)'=A_1'\cap A_2'\cap\cdots\cap A_n',$$

$$(A_1\cap A_2\cap\cdots\cap A_n)'=A_1'\cup A_2'\cup\cdots\cup A_n'.$$

证明 〈归纳基础〉 当 $n=1$ 时，结论显然成立。

当 $n=2$ 时，由德·摩根定律，结论成立。

〈归纳步骤〉 假设对任一正整数 $k\geqslant 1$，有

$$(A_1\cup A_2\cup\cdots\cup A_k)'=A_1'\cap A_2'\cap\cdots\cap A_k',$$

$$(A_1\cap A_2\cap\cdots\cap A_k)'=A_1'\cup A_2'\cup\cdots\cup A_k'.$$

则
$$\begin{aligned}(A_1\cup A_2\cup\cdots\cup A_{k+1})' &=[(A_1\cup A_2\cup\cdots\cup A_k)\cup A_{k+1}]'\\ &=(A_1\cup A_2\cup\cdots\cup A_k)'\cap A_{k+1}'\\ &=A_1'\cap A_2'\cap\cdots\cap A_k'\cap A_{k+1}',\end{aligned}$$

$$\begin{aligned}(A_1\cap A_2\cap\cdots\cap A_{k+1})' &=[(A_1\cap A_2\cap\cdots\cap A_k)\cap A_{k+1}]'\\ &=(A_1\cap A_2\cap\cdots\cap A_k)'\cup A_{k+1}'\\ &=A_1'\cup A_2'\cup\cdots\cup A_k'\cup A_{k+1}'.\end{aligned}$$

所以，对所有的正整数 n，结论成立。

例 4　试证明定理：每一正整数 $n\geqslant 2$ 可以写成素数的乘积.

证明　〈归纳基础〉当 $n=2$ 时，因为 2 是一个素数，所以定理成立。

〈归纳步骤〉设对任一正整数 $k+1>2$, 整数 $2,3,4,\cdots,k$ 都能写成素数的乘积。如果 $k+1$ 是素数，则得证。否则 $k+1=i\cdot j$，其中 $2\leqslant i\leqslant k$，$2\leqslant j\leqslant k$，根据归纳假设，i 和 j 二者都能写成素数的乘积，所以 $k+1=i\cdot j$ 也能写成素数的乘积。因此，对于所有的正整数 $n>2$，定理成立。

数学归纳法也常常是确定一个函数的比较方便的法则。下面我们用例子来说明如何应用数学归纳法的原理在自然数集或非负整数集上定义函数。

例 5　阶乘函数 $n!\,(n\geqslant 0)$ 被定义为：

$$0!=1.$$

$$(n+1)!=(n+1)\cdot n!\qquad(n=0,1,2,3,\cdots).$$

例 6　斐波拉契 (Fibonacci) 函数 F_b: $Z\to Z$ 被定义为：

$$F_b(0)=0,\ F_b(1)=1.$$

$$F_b(n+1)=F_b(n-1)+F_b(n)\qquad(n=1,2,3,\cdots).$$

对于任何的 $n\in N$ $(n\geqslant 2)$，函数值 $F_b(n)$ 可依据上式归纳到计算 $F_b(0)$ 和 $F_b(1)$。例如，求 $F_b(4)$ 时，可如下进行：

$$\begin{aligned}F_b(4)&=F_b(2)+F_b(3)\\&=F_b(0)+F_b(1)+F_b(1)+F_b(2)\\&=F_b(0)+F_b(1)+F_b(1)+F_b(0)+F_b(1)\\&=0+1+1-0+1\\&=3.\end{aligned}$$

这样，前十个斐波拉契数是 0, 1, 1, 2, 3, 5, 8, 13, 21, 34。

在第一章，我们曾介绍了集合的两种表示方法，或者用列举法，或者用描述法。我们注意到，无限集仅能用描述法，但是利

用说明元素 $a\in A$ 的定义条件，并不总是表示一个集合的便利的方法。例如全集合 U 的一组子集 $A_1, A_2, \cdots, A_r$ 所产生的所有集合的集合就不存在方便和清楚的定义条件来表示。对于这样的一些集合经常是采用归纳定义的方法来加以定义。一般说来，一个集合 S 的归纳定义由三个主要步骤组成：第一步是指定某集合 A 的元素是 S 的基本元素；第二步是指定一组规则，这些规则规定如何通过某些运算从 A 的元素求得 S 的其它元素。这一步称为归纳步；最后一步，它往往被省略，是说 S 仅仅由有限次地使用第一步和第二步而求得的那些元素组成。

例 7 求由下列定义所给出的集合：

(1) $3\in S$;

(2) 若 x、$y\in S$，则 $x+y\in S$;

(3) 集合 S 是由有限次地使用步骤 (1) 和 (2) 而得到的那些元素所组成。

解 集合 S 由 3 的所有正整数倍所组成。

例 8 给出集合 $S=\{2,3,4,\cdots\}=N-\{1\}$ 的归纳定义。

解 (1) $2\in S$，$3\in S$;

(2) 如果 x、$y\in S$，则 $x+y\in S$;

(3) 集合 S 是由有限次地使用步骤 (1) 和 (2) 而得到的那些元素所组成。

例 9 试证明：对 $n\in N$，定义在 N 上的形如 $f(x)=x+n$ 的所有函数组成的集合 S，可按下列步骤定义：

(1) $f_1(x)=x+1$ 在 S 中；

(2) 若 f，$g\in S$，则 $fg\in S$;

(3) 只有有限次地使用步骤(1)和(2)而得到的函数才在 S 中。

证明 首先，有 $f_1(x)=x+1$ 在 S 中。而且如果 $f_k(x)=x+k$，$k\in N$，是在 S 中，则

$$(f_1 f_k)(x)=f_1(x+k)=(x+k)+1=x+(k+1),$$

即 f_{k+1} 也在 S 中。所以对任意的 $n\in N$，$f(x)=x+n$ 在 S 中。

其次，如果 $f(x)=x+n_1$ 和 $g(x)=x+n_2$，则

$$(fg)(x)=f(x+n_2)=(x+n_2)+n_1=x+(n_1+n_2),$$

也具有 $x+n$ 的形式，这就保证步骤（2）只生成所求的函数。

例 10 由 $A_1, A_2, \cdots, A_r$（都是全集 U 的子集）产生的集合，可如下归纳地定义：

（1）ϕ，U，$A_1,A_2,\cdots,A_r$ 是由 $A_1,A_2,\cdots,A_r$ 产生的集合；

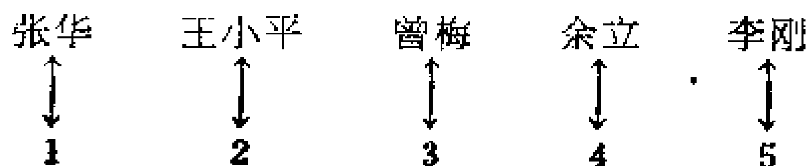
（2）如果 S 和 T 是由 $A_1, A_2, \cdots, A_r$ 产生的集合，那么（a）S'，（b）$(S\cup T)$，（c）$(S\cap T)$ 也是由 $A_1,A_2,\cdots,A_r$ 产生的集合（在 $\cap$ 优先于 $\cup$ 的约定下，括号可省略）。

根据以上定义，可以判定任一由符号，$\phi, U, A_1, A_2, \cdots, A_r, '$，$\cup,\cap$，“(” 和 “)” 所构成的表达式是否为 $A_1, A_2,\cdots, A_r$ 产生的集合.

§3.7 集合的基数

§1.1 中我们曾给出了集合的基数的概念，对于有限集来说，所谓集合的基数即为集合中不同元素的个数。但对于无限集来说，集合的基数是什么呢？是不是所有无限集的基数都一样呢？在讨论了关系和函数的概念之后，我们便能够以更严谨的方式来讨论集合的基数。

对于一个有限集合，其中不同的元素是如何进行计数的呢？例如图书馆的藏书，我们可以一册一册地清点，一个城市的人口，可以逐个登记。这些做法的实质是使这些集合的元素和自然数集的一个子集的元素建立起一一对应关系。例如，一个小组有若干个同学，我们依次点名：



就发现这个小组的成员与N的子集$\{1,2,3,4,5\}$的元素有一个一一对应，所以就说这个小组有5个同学。但是为了计数，有时并不一定要建立该集合与自然数集的某个子集的一一对应。例如，一个剧场里，如果每个观众都坐在一把椅子上，既没有站着的人，又没有空着的位子，那么观众和椅子的数目就相同。也就是说，只要知道一个集合和另一个元素个数已知的集合之间有一一对应关系，则这个集合的元素个数也知道了。这个事实启发我们如何去研究无限集的基数。因为对无限集来说，"元素的个数"这个概念是没有意义的。

定义 3-10 设有集合A、B，如果存在一个双射函数$f: A \to B$，则说A和B有**相同的基数**，或者说A与B**等势**，记作$A \sim B$。

显然，对于有限集来说，所谓A和B具有相同的基数，即是指它们的元素个数相同。

例 1 设$N_e = \{2,4,6,8,\cdots\}$，定义函数$f: N \to N_e$，使得对于任一$n \in N$，有$f(n) = 2n$。显然，f是从N到N_e的双射。所以$N \sim N_e$。

例 2 设$R_+ = \{x \mid x \in R,\ x > 0\}$，$R_1 = \{x \mid x \in R,\ 0 < x < 1\}$，定义函数$f: R_+ \to R_1$，使得对于任一$x \in R_+$，有$f(x) = \frac{x}{1+x}$。显然，$f$是从$R_+$到$R_1$的双射，所以$R_+ \sim R_1$。

注意，当$A \sim B$时，双射$f: A \to B$可能不止一个，但只要有一个双射存在，就足以证明两个集合等势。例如在例2中，我们还有另一个双射$h: R_+ \to R_1$，对于任一$x \in R_+$，$h(x) = \frac{x^2}{1+x^2}$。

定理 3-13 设S是一个集族，$\sim$是S上的一个关系，定义为当且仅当存在着一个由A到B的双射时，有$A \sim B$，则$\sim$是S上的一个等价关系。

证明 显然对于任意集合A，函数I_A是一个由A到A的双射，因此$\sim$是自反的。如果存在一个由A到B的双射$f: A \to B$，则根据定理3-4，f^{-1}是一个由B到A的双射，因此$\sim$是对称的。

如果存在一个由A到B的双射f和一个由B到C的双射g，则根据定理 3-2，gf是一个由A到C的双射，因此～是可传递的。故～是一个等价关系。证完。

于是等价关系（或称等势关系）～导致S上的一个等价分划。这个等价分划的等价类称做基数类。凡属于同一基数类的集合必有相同的基数，称作同基。

到底什么是一个集合的基数，我们并没有给出明确的回答，事实上也很难给出一个明确的回答。我们只是说基数是集合的一个性质，任何两个集合，如果它们等势，它们便有相同的基数。

定义 3-11 如果集合A与集合$N_m=\{1,2,\cdots,m\}$（m是某一正整数）属于同一基数类，则称集合A是**有限集**，$\#A=m$。$\#\phi=0$，ϕ也是有限集。不是有限集的集合称为**无限集**。

由上述定义可知，有限集的基数就是该集合中元素的个数。

无限集中最简单的一种是可数集。

定义 3-12 如果集合$A\sim N$，则称A是**可数集**。有限集和可数集总称为**可计数集**。如果集合A是无限的但不是可数的，则称A是**不可数集**。

可数集的基数记作“$\aleph_0$”，读作“阿列夫零”。

下面给出一些可数集的例子。

例 3 $N_0=\{1,3,5,7,\cdots\}=\{2n-1|n\in N\}$，定义函数$f$：$N\to N_0$，对于任一$n\in N$，$f(n)=2n-1$。显然$f$是一个双射，所以$N_0$是一个可数集。

例 4 整数集$I=\{\cdots,-3,-2,-1,0,1,2,3,\cdots\}$是一个可数集。因为我们可以把$I$的元素排成以下次序$I=\{0,1,-1,2,-2,3,-3,\cdots\}$，然后使$I$与$N$一一对应：

$$\begin{array}{cccccccc} 0 & 1 & -1 & 2 & -2 & 3 & -3 & \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \cdots \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & \end{array}$$

这个对应关系显然是一个双射。

因为正整数集N中的元素，可以排成一个无穷序列的形式，即

$$1,2,3,4,5,\cdots$$

因此，任何可数集A令与自然数n对应的元素为$a_n(n=1,2,3,\cdots)$，则A的元素按此编号也可以排成无穷序列的形式：

$$a_1,a_2,a_3,a_4,a_5,\cdots$$

反之，任一无限集合A，如果它的元素可以排成上述序列的形式，则A一定是可数集。因为我们可以令序列中的第n个元素和正整数n对应。所以一个集合是可数集的充分必要条件是它的全部元素可以排成一个无穷序列的形式。

定理3-14 任一无限集A必包含一可数子集。

证明 从A中取出一元素a_1，因A是无限集，故$A-\{a_1\}\neq\phi$。于是，在$A-\{a_1\}$中又可取一元素a_2，同理$A-\{a_1,a_2\}\neq\phi$。如此继续下去，设已从A中取出互不相同的元素：

$$a_1,a_2,a_3,\cdots,a_n,$$

则因为A为无限，所以$A-\{a_1,a_2,\cdots,a_n\}\neq\phi$。从而可以在$A-\{a_1,a_2,\cdots,a_n\}$中取一元素$a_{n+1}$，由归纳法，我们得到了一个由$A$中互不相同的元素作成的无穷序列

$$a_1,a_2,\cdots,a_n,\cdots$$

显然，$A^*=\{a_1,a_2,\cdots,a_n,\cdots\}$是可数的，且$A^*\subseteq A$。证完。

定理3-15 可数集的无限子集仍是可数集。

证明 设A_1是可数集合A的无限子集。因为$A\sim N$，所以有双射函数f：$N\to A$，于是A的元素可以排列为

$$f(1),f(2),f(3),f(4),\cdots$$

从这个序列中删去不在A_1中出现的那些元素，因为A_1为无限，剩下的元素个数必为无限。按照这些元素在序列中出现的先后次序，我们用$f(i_1)$，$f(i_2)$，$f(i_3)$，…表示它们。定义函数g：$N\to A_1$，使得对于任一$n\in N$，$g(n)=f(i_n)$，那么g是由N到A_1

的双射，所以 A_1 也是可数集。证完。

定理 3-16 设集 A 可数，集 B 有限，且 $A\cap B=\phi$，则 $A\cup B$ 可数。

证明 因集 A 可数，故 A 的元素可排成无穷序列的形式，即 $A=\{a_1,a_2,\cdots,a_n,\cdots\}$。设 B 有 m 个元素，则 $B=\{b_1,b_2,\cdots,b_m\}$，则

$$A\cup B=\{b_1,b_2,\cdots,b_m,a_1,a_2,\cdots,a_n,\cdots\}$$

可见 $A\cup B$ 的元素可排成无穷序列的形式，因而可数。证完。

定理 3-17 若 A、B 都是可数集，$A\cap B=\phi$，则 $A\cup B$ 可数。

证明 设 $A=\{a_1,a_2,a_3,\cdots\}$，$B=\{b_1,b_2,b_3,\cdots\}$，

则

$$A\cup B=\{a_1,b_1,a_2,b_2,a_3,b_3,\cdots\},$$

显然，$A\cup B$ 是可数集。证完。

定理 3-18 若 A 是可数集，B 是可数集或有限集，则 $A\cup B$ 是可数集。

证明 令 $B^*=B-(A\cap B)$，则 $A\cap B^*=\phi$，且 $A\cup B=A\cup B^*$。而由定理 3-15，B^* 是有限集或可数集，故由定理 3-16 或定理 3-17 知 $A\cup B$ 可数。证完。

定理 3-19 有限个可数集的并集仍是可数集。

证明留给读者。

定理 3-20 可数个互不相交的可数集的并集仍是可数集。

证明 设 $A_i\,(i=1,2,3,\cdots)$ 是可数集，且 $A_i\cap A_j=\phi\,(i\neq j)$。

令

$$\begin{array}{l}
A_1=\{a_{11},\rightarrow a_{12},\ a_{13},\rightarrow a_{14},\cdots\}\\
\qquad\quad\swarrow\qquad\nearrow\ \swarrow\\
A_2=\{a_{21},\ a_{22},\ a_{23},\ a_{24},\cdots\}\\
\qquad\ \downarrow\ \nearrow\ \swarrow\\
A_3=\{a_{31},\ a_{32},\ a_{33},\ a_{34},\cdots\}\\
\qquad\ \swarrow\\
A_4=\{a_{41},\ a_{42},\ a_{43},\ a_{44},\cdots\}\\
\qquad\ \downarrow\\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots
\end{array}$$

按箭头所示的次序排列元素，于是有

$$\bigcup_{i=1}^{\infty} A_i = \{a_{11}, a_{12}, a_{21}, a_{31}, a_{22}, a_{13}, a_{14}, a_{23}, \cdots\}.$$

所以 $\bigcup_{i=1}^{\infty} A_i$ 是可数集.

定理 3-21 可数个可数集的并集仍是可数集.

证明 设 $A_i (i=1,2,3,\cdots)$ 为可数集，令 $A_1^* = A_1$，$A_i^* = A_i - (A_i \cap (\bigcup_{j=1}^{i-1} A_j))$ $(i \geqslant 2)$，则 A_i^* 有限或可数，且 $A_i^* \cap A_j^* = \phi$ $(i \neq j)$。而 $\bigcup_{i=1}^{\infty} A_i = \bigcup_{i=1}^{\infty} A_i^*$，故知 $\bigcup_{i=1}^{\infty} A_i$ 是可数集. 证完.

例 5 有理数集 Q 是一个可数集.

为了证明这一结论，我们令 $A_i = \left\{\frac{1}{i}, \frac{2}{i}, \frac{3}{i}, \cdots\right\}$ $(i=1,2,3,\cdots)$，则 A_i 是可数集. 于是由定理 3-21 知所有正有理数的集合 $Q^+ = \bigcup_{i=1}^{\infty} A_i$ 是可数集. 显然所有负有理数的集合 Q^- 与 Q^+ 等势，故 Q^- 也是可数集. 而集合 $Q = Q^+ \cup Q^- \cup \{0\}$，故由定理 3-16 和 3-17 知有理数集 Q 是可数集.

并不是所有的无限集都是可数的，下面将证明实数集合是不可数集.

定理 3-22 集合 $R_1 = \{x \mid x \in R, 0 < x < 1\}$ 是不可数集.

证明 （用反证法）R_1 中任一元素必可写成无限的十进小数 $0.a_1a_2\cdots a_n\cdots$，其中 a_i 是 $0,1,2,\cdots,9$ 中某个数. 这里我们规定，所有的有限小数都写成以 9 为循环节的循环小数.（例如 0.243 要写成 0.24299⋯）这样的规定使得每一个小数都只有唯一的一种小数表示法. 现设 R_1 是可数集，则它的元素可编号如下：

$$a_1 = 0.a_{11}a_{12}a_{13}\cdots a_{1n}\cdots,$$
$$a_2 = 0.a_{21}a_{22}a_{23}\cdots a_{2n}\cdots,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$a_n = 0.a_{n1}a_{n2}a_{n3}\cdots a_{nn}\cdots,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$

而一切适合 $0<x<1$ 的实数应该完全在其中。现在我们构造一个新的实数 $b=0.b_{11}b_{22}b_{33}\cdots b_{nn}\cdots$，其中

$$b_{ii}=\begin{cases}1 & a_{ii}\neq 1,\\ 2 & a_{ii}=1.\end{cases}$$

所以 $b_{ii}\neq a_{ii}$，且 b 也是 $(0,1)$ 区间的一个数，即 $b\in R_1$，但显然 b 与所有实数 $a_1, a_2, a_3,\cdots$ 都不相同，因此 $b\notin R_1$。这就产生了矛盾，所以 R_1 是一个不可数集。证完。

这里的证明方法，称为“对角线证法”。因为它是比照着上表中对角线上的元素 a_{ii} 来作 b_{ii} 的。

定理 3-22 说明集合 R_1 与正整数集 N 属于不同的基数类。我们用“$\aleph_1$”表示 R_1 的基数，并称“$\aleph_1$”为**连续基数**。

定理 3-23 实数集 R 是不可数集。并且它的基数就是连续基数。

证明 定义函数 $f: R_1\to R$，

$$f(x)=\begin{cases}\dfrac{1}{2x}-1 & 0<x\leqslant\dfrac{1}{2},\\[2ex] \dfrac{1}{2(x-1)}+1 & \dfrac{1}{2}<x<1.\end{cases}$$

这是一个由 R_1 到 R 的双射，因此 R 也是不可数集，且具有连续基数 $\aleph_1$。证完。

在有限集与无限集之间存在着一个重要的差别，这就是任何有限集都不可能与它的真子集等势。因为从一个有限集合 A 到 A 的真子集无法建立起双射函数的关系。但是任何无限集都能够与它的一个真子集等势（证明留给读者）。于是我们看到，无限集具有的这种性质，是有限集所没有的。因此我们又可以用它来作为无限集的定义。

由上讨论可知，虽然都是无限集，但它们可能有互不相同的基数。那么各个集合的不同基数之间是否有大小关系呢？由于基

数的概念是“元素个数”这一概念的推广，因此我们给出下述定义。

定义 3-13 设有集合 A、B，若 $A \nsim B$（即不等势），但 A 与 B 的某个真子集等势，则称 A 的基数小于 B 的基数，记作 $\#A < \#B$ 或 $\#B > \#A$。

显然，这个定义确实是有限集合 A 的元素个数小于有限集合 B 的元素个数这一概念的推广。

注意，上述定义中的 $A \nsim B$ 的限制是不可少的，因为若 A 是无限集，则它可以和它的一个真子集等势，如果取 $A = B$，则 A 与 B 的一个真子集等势。可是我们当然不应该得出结论 $\#A < \#A$。因此必须加上 $A \nsim B$ 这样的限制。在加上了这样的限制后，我们可以证明 $\#A = \#B$，$\#A < \#B$，$\#A > \#B$ 不可能有两个同时成立。显然，根据定义 $\#A = \#B$ 和 $\#A < \#B$，$\#A = \#B$ 和 $\#A > \#B$ 不会同时成立。为了断定 $\#A < \#B$ 和 $\#A > \#B$ 不可能同时成立，就必须证明在 A 和 B 不等势的前提下，不可能既有 A 的真子集 A_1 与 B 等势，又有 B 的真子集 B_1 与 A 等势。

定理 3-24 设 A、B 是两个集合，若有 A 的子集 A_1 和 B 的子集 B_1 使得 $A \sim B_1$，$B \sim A_1$，则 $A \sim B$。

证明省略。

定理3-14说明可数集的基数是无限集的基数中的最小者。特别有 $\aleph_0 < \aleph_1$。

我们知道，对于任一有限集 A，如果 A 的基数 $\#A = n$，则 A 的幂集 2^A 的基数 $\#(2^A) = 2^n$。因此任意一个有限集 A 的基数必然小于集合 2^A 的基数。那么对于任一给定的无限集，是否也可以找到另一个集合使其基数大于给定集合的基数呢？下面的定理说明这样的集合是存在的。

定理 3-25 对于任何集合 A，有 $\#A < \#(2^A)$

证明 定义函数 f：$A \to 2^A$，使得对于每个 $a \in A$，$f(a) = \{a\}$。

显然 f 是内射，但不是满射。即 f 是由 A 到 2^A 的一个真子集的双射。为了证明 $A \not\sim 2^A$，我们假设存在一个双射 $g: A \to 2^A$，对于每一个元素 $a \in A$，如果 $a \in g(a)$，则我们称 a 为 A 的"内元素"，如果 $a \notin g(a)$，则称 a 为 A 的"外元素"。设 B 是 A 中所有外元素的集合，即

$$B = \{x \mid x \in A,\ x \notin g(x)\}$$

显然 $B \subseteq A$，所以 $B \in 2^A$，因为 g 是双射，必存在一元素 $b \in A$，使得 $g(b) = B$。现有两种情况，或者 $b \in B$，则 b 是一个内元素，这与 B 的定义矛盾；或者 $b \notin B$，则 b 是一个外元素，因而 $b \in B$，这又是一个矛盾。所以不存在由 A 到 2^A 的双射，即 $A \not\sim 2^A$。从而有 $\#A < \#(2^A)$。证完。

上述定理说明，无论一个集合的基数多么大，一定有更大基数的集合存在。即不可能存在一个最大的基数。

§3.8 整数的基本性质

我们知道，任意两个整数可以相加、相减和相乘，其结果仍是整数。但两个整数不一定可以在整数的范围内相除。研究整数的性质基本上就是研究整除性，素因子分解以及和这些有关的问题。

定理 3-26 设 a、b 是两个整数，$b \neq 0$，则必有二整数 q 及 r 存在，使得

$$a = qb + r,\quad 0 \leqslant r < |b|,$$

且 q 及 r 是唯一存在的。

证明 我们用符号 $[\alpha]$ 表示不超过 α 的最大整数，于是，显然有 $[\alpha] \leqslant \alpha < [\alpha] + 1$。

先证明 q 与 r 的存在性．因为 $\left[\frac{a}{|b|}\right]\leqslant\frac{a}{|b|}<\left[\frac{a}{|b|}\right]+1$，所以 $0\leqslant\frac{a}{|b|}-\left[\frac{a}{|b|}\right]<1$，从而 $0\leqslant a-\left[\frac{a}{|b|}\right]\cdot|b|<|b|$．于是，当 $b>0$ 时，$a=\left[\frac{a}{|b|}\right]\cdot b+\left(a-\left[\frac{a}{|b|}\right]\cdot|b|\right)$；当 $b<0$ 时，$a=\left(-\left[\frac{a}{|b|}\right]\right)\cdot b+\left(a-\left[\frac{a}{|b|}\right]\cdot|b|\right)$．这说明 q 和 r 是存在的．

现在来证明 q、r 的唯一性．若 $a=qb+r=q_1b+r_1$ $(0\leqslant r_1<|b|)$，则 $r_1-r=(q-q_1)b$，但由于 $0\leqslant|r_1-r|<|b|$，就应该有 $0\leqslant|(q-q_1)b|=|q-q_1|\cdot|b|<|b|$．所以 $0\leqslant|q-q_1|<1$（$\because b\neq0$），于是不得不有 $q=q_1$，因此也就有 $r=r_1$．定理得证．

定理 3-26 中的 q 和 r 就是通常所说的用 b 除 a 所得的商和余数。若余数 $r=0$，就说 b 整除 a．

定义 3-14 对于任意两个整数 a 和 $b\neq0$，若存在一个整数 c，使得 $a=bc$，则说 b 能整除 a 或 a 能被 b 整除；也说 a 是 b 的**倍数**，b 是 a 的**因数**．记作 $b|a$．若 b 不能整除 a，则记作 $b\nmid a$．

例如，任一非零整数整除 0，而 ±1 整除任意整数．

由整除的定义，很容易证明下面几条简单的性质：

1）若 $a|b$，$b|c$，则 $a|c$．

证明 因为 $a|b$，$b|c$，故有整数 d，e 使 $b=ad$，$c=be$，因此 $c=a(de)$，而 de 为整数，所以 $a|c$．

2）若 $a|b$，则对于任意整数 c，$a|bc$．

证明 由定义，$b|bc$，又由假设 $a|b$，故由 1）有 $a|bc$．

3）若 $a|b$，$a|c$，则对任意的整数 m、n，有 $a|mb\pm nc$．

证明 因为 $a|b$，$a|c$，故有整数 d，e 使 $b=ad$，$c=ae$，所以，$mb\pm nc=mad\pm nae=a(md\pm ne)$，而 $md\pm ne$ 为整数，所以 $a|mb\pm nc$．

4）若在一个等式中，除某一项外，其余各项都是 a 的倍数，则此项也是 a 的倍数．

证明 设在等式 $b_1+b_2+\cdots+b_n=c_1+c_2+\cdots+c_m$ 中，b_2，$\cdots$，b_n，c_1，c_2，$\cdots$，c_m 都是 a 的倍数，解出 $b_1=c_1+c_2+\cdots+c_m-b_2-b_3-\cdots-b_n$，由 3) $c_1+c_2+\cdots+c_m-b_2-b_3-\cdots-b_n$ 是 a 的倍数，故 b_1 是 a 的倍数。

5) 若 $a|b$，$b|a$，则 $b=\pm a$

证明 因为 $a|b$，$b|a$，则有整数 d，e 使得 $b=ad$，$a=be$，于是 $a=ade$，消去 a 得 $1=de$，而 d，e 都是整数，相乘得 1，故 d 和 e 都等于 ±1，因而 $b=\pm a$。

定义 3-15 如果 c 是 a 的因数，同时又是 b 的因数，则称 c 是 a 和 b 的**公因数**。

显然，对于任意整数 a，b，±1 是它们的公因数。

因为一个不等于 0 的整数的因数的绝对值不大于这个数本身的绝对值，所以两个整数 a，b（其中至少有一个不等于 0）的公因数的绝对值当然也不大于 a、b 中不等于 0 的整数的绝对值。于是，a 与 b 的公因数的个数一定是有限多个，因此它们当中必有一个最大的。

定义 3-16 整数 a 和 b 的公因数中最大的一个称为是 a，b 的**最大公因数**，用符号 (a, b) 表示。

于是由定义就知道，最大公因数是正整数。

若 a，b 中有一个是 0，则另一个的绝对值就是它们的最大公因数。若 $a\neq0$，$b\neq0$，但 $b|a$，则 $|b|$ 就是 a，b 的最大公因数；若 $b\nmid a$，则以 b 除 a 得商 q 和余数 r，而

$$a=qb+r,\ 0<r<|b| \qquad (3\text{-}1)$$

观察（3-1）式我们发现，若 d 是 b 和 r 的公因数，则由 4)，d 也是 a 的因数，因而是 a，b 的公因数。反之，若 d 是 a 和 b 的公因数，则由 4)，d 也是 r 的因数，因而是 b，r 的公因数。由此可见，a，b 的公因数和 b，r 的公因数完全是相同的。因此为了求 a，b 的最大公因数，只要求 b，r 的最大公因数就行了。若 $r|b$，

则 r 就是 b, r 的最大公因数. 因而也就是 a, b 的最大公因数；若 $r\nmid b$, 则以 r 除 b 得商及余数…，如此作下去. 因为所得的余数逐次减少，所以最后必将获得一个余数为 0 的式子. 这就是所谓辗转相除法. 设用辗转相除法得到的各式为：

$$\begin{cases} a = q_1 b + r_1; \\ b = q_2 r_1 + r_2; \\ r_1 = q_3 r_2 + r_3; \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ r_{n-2} = q_n r_{n-1} + r_n; \\ r_{n-1} = q_{n+1} r_n. \end{cases} \tag{3-2}$$

由以上的推理我们知道，a, b 的公因数和 b, r_1 的公因数相同，和 r_1, r_2 的公因数相同，…，和 r_{n-1}, r_n 的公因数相同. 因此有

$$(a,b)=(b,r_1)=(r_1,r_2)=\cdots=(r_{n-2},r_{n-1})=(r_{n-1},r_n),$$

但由（3-2）的最后一式知 $r_n \mid r_{n-1}$, 故 $(r_{n-1},r_n)=r_n$, 因此 $(a,b)=r_n$.

例 1 设 $a=6099$ $b=2166$. 求 (a, b).

解 因为 $6099 = 2\cdot 2166 + 1767$

$2166 = 1\cdot 1767 + 399$

$1767 = 4\cdot 399 + 171$

$399 = 2\cdot 171 + 57$

$171 = 3\cdot 57$

所以 $(6099, 2166) = 57$

定理 3-27 设 a 和 b 是两个整数，且 $(a,b)=d$, 则存在整数 s 和 t, 使得 $d=sa+tb$.

证明 令 J 是可以写成 $ma+nb$（m, n 为整数）的全部正整数的集合，即

$$J=\{ma+nb \mid m,n \text{ 为整数}, \ ma+nb>0\}.$$

因为 J 非空（a 和 $-a$ 二者必有其一属于 J），所以它有一个最小元素，设为 k，并令 $k=m_0a+n_0b$，如果 $a=h_1d$，$b=h_2d$，则我们有

$$k=m_0a+n_0b=m_0h_1d+n_0h_2d=d(m_0h_1+n_0h_2),$$

这意味着 $$d\leqslant k. \tag{3-3}$$

另一方面，根据定理 3-26，我们能够写出 $a=qk+r$，这里 $0\leqslant r<k$，所以

$$r=a-qk=a-q(m_0a+n_0b)=(1-m_0q)a+(-n_0q)b.$$

这意味着或者 $r=0$，或者 $r\in J$，但由于 $r<k$，而 k 是 J 中最小的元素，因此必有 $r=0$，所以 k 是 a 的因数。同样的道理可以证明 k 是 b 的因数。因此 k 是 a 和 b 的公因数，于是有

$$k\leqslant d. \tag{3-4}$$

由 (3-3) 和 (3-4) 可知，$d=k$。故定理得证。

例 2 以 $a=6099$ 和 $b=2166$ 为例，我们来说明整数 s 和 t 的计算。

由例 1 我们能够写出

$$\begin{aligned}57&=399-2\cdot171\\&=399-2(1767-4\cdot399)=-2\cdot1767+9\cdot399\\&=-2\cdot1767+9(2166-1\cdot1767)=9\cdot2166-11\cdot1767\\&=9\cdot2166-11(6099-2\cdot2166)=-11\cdot6099+31\cdot2166,\end{aligned}$$

所以 $$(6099,2166)=-11\cdot6099+31\cdot2166.$$

定理 3-28 整数 a, b 的任一公因数是它们的最大公因数的因数。

证明 设 c 是 a, b 的任一公因数，因为 $(a,b)=sa+tb$，所以由 $c|a$，$c|b$，即得 $c|(sa+tb)$。也就是 $c|(a,b)$。证完。

类似地，对于任意有限个整数 $a_1,a_2,\cdots,a_n$，只要这 n 个数中有一个不等于零，我们同样可以定义这 n 个数的最大公因数，仍用符号 $(a_1,a_2,\cdots,a_n)$ 表示 $a_1,a_2,\cdots,a_n$ 的最大公因数。如果

$(a_1, a_2, \cdots, a_n) = 1$，就称 $a_1, a_2, \cdots, a_n$ 是**互素**的。特别当 $a_1, a_2, \cdots, a_n$ 中每一个都和另一个互素时（即对所有的 $i \neq j$，$(a_i, a_j) = 1$，$i, j = 1, 2, \cdots, n$），称 $a_1, a_2, \cdots, a_n$ 是**两两互素**的。显然，两两互素的数一定是互素的，但互素的诸数却不一定是两两互素的。例如，整数 6，9 和 11 是互素的，但却不是两两互素的。整数 5、9 和 11 是两两互素的。当然，对于两个整数来说，互素和两两互素这两个概念是一致的。

定理 3-29 若 a，b 互素，而 $a|bc$，则 $a|c$。

证明 因为 a，b 互素，故由定理 3-27 有整数 s，t，使 $1 = sa + tb$，因而 $c = sac + tbc$，但 $a|sac$，$a|tbc$，因此 $a|c$，证完。

定义 3-17 一个大于 1 的正整数，如果除了 1 和它自身以外，没有其它正因数，则称该正整数为**素数**（或称质数）。

定理 3-30 若 p 为素数而 $p|a_1a_2\cdots a_n$，则 p 必整除 $a_1, a_2, \cdots, a_n$ 之一。

证明 若 $p|a_n$，则定理得证。若 $p\nmid a_n$，则 p 不是 a_n 的因数，但 p 只有 1 和 p 两个正因数，故 p 和 a_n 的最大公因数是 1，即 p 和 a_n 互素，由 $p|(a_1a_2\cdots a_{n-1})a_n$ 及定理 3-29，$p|a_1a_2\cdots a_{n-1}$。同样，若 $p|a_{n-1}$，则定理得证，否则必有 $p|a_1a_2\cdots a_{n-2}$，如此类推，必可找到 $a_n, a_{n-1}, \cdots, a_1$ 中的一个为 p 整除。证完。

定理 3-31 （素因数分解定理）

每个整数 $n \geqslant 2$ 恰有一种方法写成素数的乘积（不论素因数出现的先后次序）。

证明 §3.6 例 4 中我们已用归纳法证明了每个整数 $n \geqslant 2$ 可以写成素数的乘积。现只要证明这种素数乘积形式的唯一性。

设
$$n = p_1p_2\cdots p_h = q_1q_2\cdots q_k \tag{3-5}$$
这里 $p_1, p_2, \cdots, p_h, q_1, q_2, \cdots, q_k$ 都是素数，且可假定 $p_1 \leqslant p_2 \leqslant \cdots \leqslant p_h$，$q_1 \leqslant q_2 \leqslant \cdots \leqslant q_k$。我们的目的是要证明 $h = k$ 且 $p_i = q_i$ $(i = 1, 2, \cdots, h)$。

首先，当n为素数时（即$n=2$或为奇素数），由素数的定义即知$h=k=1$，$p_1=q_1=n$，于是定理成立。

现设n不是素数（因此$n>2$），并假设定理对于小于n的数都成立。由于n不是素数，必有$h>1$，$k>1$.因为$q_1|p_1p_2\cdots p_h$，$p_1|q_1q_2\cdots q_k$，根据定理3-30，必有$q_1|p_j$（$1\leqslant j\leqslant h$），$p_1|q_l$（$1\leqslant l\leqslant k$），因为p_j也是素数，它只有p_j和1两个正因数，而$q_1\neq1$，故必有$q_1=p_j$。同样的道理，必有$p_1=q_l$。因此得到$q_1=p_j\geqslant p_1$，$p_1=q_l\geqslant q_1$，故不得不有$p_1=q_1$。在（3-5）式中消去p_1，得

$$p_2p_3\cdots p_h=q_2q_3\cdots q_k<n,$$

根据归纳假设知$h-1=k-1$，因此$h=k$,且$p_i=q_i$（$i=2,3,\cdots,h$），又由前面已证$p_1=q_1$，因此唯一性得证。

定理3-32 对于任意整数$n\geqslant1$和$b\geqslant2$，n能够唯一地表示成以下形式：

$$n=a_0+a_1b+a_2b^2+\cdots+a_kb^k, \tag{3-6}$$

其中$0\leqslant a_i<b$（$i=0,1,\cdots,k$）且$a_k\neq0$。

证明 （对n进行归纳）

当$n=1$时，取$a_0=1,k=0$，我们得到$n=1$。这便是（3-6）式所给出的形式。由于$b\geqslant2$，因此上述形式是唯一的。

假设对于整数$1,2,\cdots,m-1$，定理成立。根据定理3-26，我们能够唯一地写出

$$m=qb+r,\ 这里\ 0\leqslant r<b.$$

因为$b\geqslant2$，因此有$q<m$，由归纳假设，我们能唯一地写出

$$q=a_0'+a_1'b+a_2'b^2+\cdots+a_k'b^k,$$

这里$0\leqslant a_i'<b$（$i=0,1,\cdots,k$）且$a_k'\neq0$。

因此，我们能够唯一地写出

$$\begin{aligned}m&=r+a_0'b+a_1'b^2+\cdots+a_k'b^{k+1}\\&=a_0+a_1b+a_2b^2+\cdots+a_{k+1}b^{k+1},\end{aligned}$$

这里，$0 \leqslant a_i < b$ $(i=0,1,\cdots,k+1)$ 和 $a_{k+1} \neq 0$。证完。

(3-6) 式中的整数 b 可看作是该表达式的基，当基事先知道（如十进制中的 10 或二进制中的 2），(3-6) 式就缩写成通常的形式 $a_k a_{k-1} \cdots a_1 a_0$。

例 3 把十进制数 427 表示成八进制数。

解 利用定理 3-32，取 $b=8$，将十进制数 427 写成 (3-6) 式的形式：

$$427 = a_0 + a_1 8 + a_2 8^2 + \cdots + a_k 8^k,$$

逐步找出上式中的 a_i，注意到

$$427 = a_0 + 8(a_1 + a_2 8 + \cdots + a_k 8^{k-1}).$$

因此，a_0 是 8 除 427 所得的余数，$427 = 53 \cdot 8 + 3$。

所以

$$a_0 = 3,$$

而且

$$53 = a_1 + a_2 8 + \cdots + a_k 8^{k-1} = a_1 + 8(a_2 + a_3 8 + \cdots + a_k 8^{k-2}).$$

同样，a_1 是 8 除 53 所得的余数，$53 = 6 \cdot 8 + 5$。

所以 $$a_1 = 5,$$

而且 $$6 = a_2 + a_3 8 + \cdots + a_k 8^{k-2}$$

显然 $$a_2 = 6.$$

由上可知，十进制数 427 可表示成八进制数 653。

习　　题

1. 以下关系中哪一个构成函数?

(1) $\{(n_1,n_2)\mid n_1,n_2\in N,\ n_1+n_2<10\}$;

(2) $\{(n_1,n_2)\mid n_1,n_2\in N,\ n_2=$ 小于 n_1 的素数的个数$\}$.

2. 设$A=2^U\times 2^U$, $B=2^U$, 给定由A到B的关系

$$f=\{((S_1,S_2),\ S_1\cap S_2)\mid S_1,S_2\subseteq U\},$$

f是函数吗? 若是的话, f的值域$R_f=2^U$吗? 为什么?

3. 下列集合能够定义函数吗? 如果能, 试指出它们的定义域和值域?

(1) $\{(1,(2,3)),\ (2,(3,4)),\ (3,(1,4)),\ (4,(1,4))\}$;

(2) $\{(1,(2,3)),\ (2,(3,4)),\ (3,(3,2))\}$;

(3) $\{(1,(2,3)),\ (2,(3,4)),\ (1,(2,4))\}$;

(4) $\{(1,(2,3)),\ (2,(2,3)),\ (3,(2,3))\}$.

4. 在下列函数中, 确定哪些是内射, 哪些是满射, 哪些是双射.

(1) f_1: $N\to Z$, $f_1(n)=$ 小于n的完全平方数的个数;

(2) f_2: $R\to R$, $f_2(r)=2r-15$;

(3) f_3: $R\to R$, $f_3(r)=r^2+2r-15$;

(4) f_4: $N^2\to N$, $f_4(n_1,n_2)=n_1^{n_2}$;

(5) f_5: $N\to R$, $f_5(n)=\log_{10}n$;

(6) f_6: $N\to Z$, $f_6(n)=$ 等于或大于$\log_{10}n$的最小整数;

(7) f_7: $(2^U)^2\to(2^U)^2$, $f(S_1,S_2)=(S_1\cup S_2,S_1\cap S_2)$.

5. 设A和B都是有限集, $\#A=n$, $\#B=m$. 问存在着多少个不同的内射f: $A\to B$? 存在多少个不同的双射?

6. 在下列函数中，确定哪些是内射，哪些是满射，哪些是双射。

(1) f_1: $I \to I$, $f_1(i) = \begin{cases} \frac{i}{2} & i\text{是偶数} \\ \frac{(i-1)}{2} & i\text{是奇数;} \end{cases}$

(2) f_2: $Z_7 \to Z_7$, $f_2(x) = \text{res}_7(3x)$;

(3) f_3: $Z_6 \to Z_6$, $f_3(x) = \text{res}_6(3x)$.

7. 设 $A = \{a_1, a_2, \cdots, a_n\}$，试证明任何从 A 到 A 的函数，如果它是内射，则它必是满射。反之亦真。

8. 设函数 f: $Z \times Z \to Z$, g: $Z \times Z \to Z$. 这里 $f(x, y) = x + y$, $g(x, y) = xy$. 试证明 f 和 g 是满射，但都不是内射。

9. 设有函数 f:$R \to R$ 和 g:$R \to R$，这里 $f(x) = x^2 - 2$ 和 $g(x) = x + 4$。求出 $f \cdot g$ 和 $g \cdot f$. 并说明这些函数是否是内射，满射或双射。

10. 设有函数 f, g, h: $R \to R$，给定为 $f(x) = x + 2$, $g(x) = x - 2$, $h(x) = 3x$，试求出 $g \cdot f$, $f \cdot g$, $f \cdot f$, $f \cdot h$, $h \cdot g$, $f \cdot h \cdot g$.

11. 设 $A = \{1, 2, 3, 4\}$，定义一个函数 f: $A \to A$，使得 $f \neq I_A$，而且是双射。求 f^2, f^3, f^{-1} 以及 $f \cdot f^{-1}$。能否找到一个双射 g: $A \to A$，使 $g \neq I_A$，但 $g^2 = I_A$?

12. 设 f: $R \to R$, $f(x) = x^3 - 2$. 试求 f^{-1}.

13. 完成定理 3-3 的证明，并相对定理 3-2 的不可逆部分举出反例。

14. 求出下列置换的逆置换 P_1^{-1} 和 P_2^{-1}，并求出 P_1P_2、P_2P_1、$(P_1 \cdot P_2P_1)^2$.

$$P_1 = \begin{pmatrix} a & b & c & d & e & f & g \\ g & f & e & d & c & b & a \end{pmatrix}, \quad P_2 = \begin{pmatrix} a & b & c & d & e & f & g \\ e & g & f & b & a & c & d \end{pmatrix}.$$

15. 已知函数 f: $A \to B$. 这里 $f(a) = 0 \cdot e_{A_1}(a) + 1 \cdot e_{A_2}(a)$ ($\{A_1, A_2\}$ 是 ρ_f 导致的 A 上的等价分划)。函数 g: $A \to C$，这里 $g(a) = 0 \cdot e_{A_3}(a) + 1 \cdot e_{A_4}(a) + 3 \cdot e_{A_5}(a)$ ($\{A_3, A_4, A_5\}$ 是 ρ_g 导致的 A 上的等价分划)。试证明：

$$f(a)+g(a)=0\cdot e_{A_1\cap A_3}(a)+e_{A_1\cap A_4}(a)+e_{A_2\cap A_3}(a)+2e_{A_2\cap A_4}(a)$$
$$+3e_{A_1\cap A_5}(a)+4e_{A_2\cap A_5}(a).$$

16. 设 $S=(A\cap B)\cup(A'\cap C)\cup(B\cap C)$，这里 A,B 和 C 是全集 U 的子集。根据 $e_A(u)$，$e_B(u)$ 和 $e_C(u)$ 的值的所有可能的组合，把 $e_S(u)$ 的值列成表。构造 S 的成员表，并将所构造的两表相比较。

17. 设 $A_1,A_2,\cdots,A_r$ 是全集 U 的子集。S 是一个由 $A_1,A_2,\cdots,A_r$ 产生的集合，S 的最小集标准形式为 $S=\bigcup\limits_{i=1}^{k}M_i$（这里 M_i 是由 $A_1,A_2,\cdots,A_r$ 产生的最小集）。试证明 $e_s(u)=\sum\limits_{i=1}^{k}e_{M_i}(u)$。

18. 如果集合 A 和 B 都是可数集，试证明集合 $A\times B$ 也是可数集。

19. 如果 A 是可数集，试证明 A^n 也是可数集。

20. 证明区间 $(0,1)$ 和 $[0,1]$ 是等势的。

21. 证明全体无理数的集合是不可数集。

22. 证明任一无限集都包含有一个与它自身等势的真子集。

23. 设 f 是由 A 到 B 的函数，$\#A>\#B$。

(1) 当 $\#A$ 除以 $\#B$ 时，设 i 是商，r 是余数，证明：

$$\left\lceil\frac{\#A}{\#B}\right\rceil=\begin{cases}i+1 & 若\ r\neq 0,\\ i & 若\ r=0.\end{cases}$$
（$\lceil x\rceil$ 表示不小于 x 的最小整数）

(2) 证明在 A 中存在 j 个元素 $a_1,a_2,\cdots,a_j$，$j=\left\lceil\frac{\#A}{\#B}\right\rceil$，使得 $f(a_1)=f(a_2)=\cdots=f(a_j)$。

24. 对 n 应用归纳法证明以下命题：

(1) $\sum\limits_{i=1}^{n}(2i-1)=n^2$；

(2) $\sum\limits_{i=1}^{n}i^2=\frac{1}{6}n(n+1)(2n+1)$；

(3) $\sum\limits_{i=1}^{n}i^3=\left[\frac{1}{2}n(n+1)\right]^2$；

(4) $\sum\limits_{i=1}^{n}i(i!)=(n+1)!-1$；

(5) 如果 f 是一个幂等函数，则 $f^n = f$；

(6) 对于任何一个满足 $0<a<1$ 的 a，

$$(1-a)^n \geqslant 1-na \qquad (n\geqslant 1);$$

(7) $2^n > n^3 (n\geqslant 10)$（提示：$(n+1)^3 = \left(1+\frac{1}{n}\right)^3 n^3$）。

25. 归纳地定义下面函数：

$$E(i) = C_n^i \qquad (i\geqslant 0).$$

26. 阿克曼 (Ackerman) 函数 A: $Z^2 \to Z$ 归纳地定义如下：

$$A(0,n) = n+1 \qquad (n\geqslant 0),$$
$$A(m,0) = A(m-1,1) \qquad (m>0),$$
$$A(m,n) = A(m-1, A(m,n-1)) \qquad (m>0, n>0).$$

计算 $A(2,3)$。

27. 设有函数 f: $I\to I$，这里 $f(i) = 2i+1$，给出函数 f^n 的表达式，并用对 n 进行归纳的方法证明这个表达式的正确性。

28. 对于下列 a 和 b 的值，计算 (a,b) 并以 $sa+tb$ 的形式表达它们：

(1) $a=14$，$b=35$；

(2) $a=180$，$b=252$；

(3) $a=4148$，$b=7684$。

29. 证明：如果 $(a,b)=d$，$(c,b)=1$，则 $(ac,b)=d$。因此，若 a，c 都和 b 互素，则 ac 也和 b 互素。

30. 证明：若 $c>0$，则 $(a,b)\cdot c = (ac,bc)$。

31. 证明：若 $(a,b)=d$，则 $\left(\frac{a}{d}, \frac{b}{d}\right)=1$。反之，若 d 是 a，b 的一个正公因数且 $\left(\frac{a}{d}, \frac{b}{d}\right)=1$，则 $(a,b)=d$。

第四章 代数系统

在这一章，我们引入代数系统的概念，说明什么是代数系统，介绍几个熟悉的代数系统的例子，并讨论它们的基本性质。这些例子表明，不同的代数系统可以具有一些共同的性质，由此说明研究抽象的代数系统的必要性。我们还将介绍一些与代数系统相关联的，重要而有用的概念，如同态、同构、同余以及代数系统的直积等。

代数系统的概念在计算机科学的许多理论领域都是必不可少的。

§4.1 运　　算

上一章我们讨论了从集合A到集合B的一般的函数。现在我们把讨论局限于从集合A^n到集合A的函数f：$A^n \to A$。由函数的定义，对于A^n中的每一个有序n元组，在A中都有唯一的元素与之对应，因为A^n的每个有序n元组$(a_1, a_2, \cdots, a_n)$中的所有$a_i \in A$，所以，函数关系$f(a_1, a_2, \cdots, a_n) = a$就可以看作是集合$A$中的$n$个元素经过某种运算$f$后在$A$中得到运算结果$a$。显然，这种运算对于集合$A$中任意$n$个元素都可进行。于是我们给出下面的定义。

定义4-1　设有集合A，函数f：$A^n \to A$称为A上的一个**n元运算**。n称为这个**运算的阶**。

特别，若函数f：$A^2 \to A$，则f是A上的二元运算。若f：$A \to A$，则f是A上的一元运算。这是两种最常见的运算。

例1　设$A = I$，可如下定义集合I上的一元和二元运算：

一元运算～：$I \to I$，对于每一个非零整数$i \in I$，$\sim(i) = -i$，$\sim(0)=0$。于是$\sim(2) = -2$，$\sim(-3)=3$，$\sim(5) = -5$。这就是通常的求相反数的运算。

二元运算＋：$I^2 \to I$，其中$+(i_1, i_2) = i_1 + i_2$，即$i_1 + i_2$是二元组(i_1, i_2)在＋运算下的象。于是$+(3,5)=3+5=8$，$+(4,-6) = 4+(-6) = -2$。这就是通常数的加法运算。

事实上，加、减、乘都是整数集合上，也是实数集合上的二元运算，但除不是这些集合上的二元运算。加和乘都是自然数集上的二元运算，但减不是自然数集上的二元运算。集合的并和交运算是全集合U的幂集2^U上的二元运算，也是任一集合的幂集上的二元运算。补运算是这些集合上的一元运算。

我们常常以特殊的符号来表示一元和二元运算。如～，$*$，$\circ$，$+$，$-$，$\cup$，$\cap$等等。对于一元运算，常将运算符号放在$a_i \in A$的前面或上面，以表示在此运算下a_i的象。对于二元运算，常将运算符号放在a_i和a_j之间，以表示在此运算下(a_i, a_j)的象。例如，$f(a_i, a_j)$可写成$a_i f a_j$或$a_i * a_j$。

当A是有限集时，例如$A = \{a_1, a_2, \cdots, a_n\}$，则$A$上的一元和二元运算常分别用形如表 4-1 的两个运算表来定义。

表 4-1

a_i	$\circ(a_i)$
a_1	$\circ(a_1)$
a_2	$\circ(a_2)$
$\vdots$	$\vdots$
a_n	$\circ(a_n)$

$\circ$	a_1	a_2	$\cdots$	a_n
a_1	$\circ(a_1, a_1)$	$\circ(a_1, a_2)$	$\cdots$	$\circ(a_1, a_n)$
a_2	$\circ(a_2, a_1)$	$\circ(a_2, a_2)$	$\cdots$	$\circ(a_2, a_n)$
$\vdots$	$\vdots$	$\vdots$		$\vdots$
a_n	$\circ(a_n, a_1)$	$\circ(a_n, a_2)$	$\cdots$	$\circ(a_n, a_n)$

如果作用在一个集合的元素上的运算，其运算结果也仍然是这同一集合中的元素，那么就称这个集合在这种运算下是封闭的。显然，集合A在其上所定义的n元运算下是封闭的。

假设在集合 A 上定义了一个 n 元运算 $\circ$，S 是 A 的一个子集，由运算 $\circ$ 的定义，S 中任意 n 个元素经过运算 $\circ$ 后，所得的运算结果是集合 A 中的元素，但不一定是 S 中的元素，即虽然 $(a_1, a_2, \cdots a_n) \in S^n$，但不能保证 $\circ(a_1, a_2, \cdots, a_n) \in S$。于是我们给出下面的概念。

定义 4-2 设 $\circ$ 是集合 A 上的一个 n 元运算，$S \subseteq A$，如果对于每一个 $(a_1, a_2, \cdots, a_n) \in S^n$，都有 $\circ(a_1, a_2, \cdots, a_n) \in S$，则称 S 在运算 $\circ$ 下是**封闭的**。

例 2 正整数集 N 上定义了二元运算加：$+(n_1, n_2) = n_1 + n_2$，令

$$N_e = \{2k \mid k \in N\} = \{2, 4, 6, 8, \cdots\};$$

$$S = \{n \mid n \in N,\ n \text{整除} 30\} = \{1, 2, 3, 5, 6, 10, 15, 30\}.$$

显然 N_e 和 S 都是 N 的子集，N_e 对二元运算 $+$ 是封闭的，但 S 对运算 $+$ 不封闭。

定理 4-1 设 $\circ$ 是定义在集合 A 上的一个 n 元运算，S_1 和 S_2 是 A 的在运算 $\circ$ 下封闭的子集，则 $S_1 \cap S_2$ 在 $\circ$ 下也是封闭的。

证明 对任一组元素 $a_1, a_2, \cdots, a_n \in S_1 \cap S_2$，因为 $a_1, a_2, \cdots, a_n \in S_1$，且 S_1 在运算 $\circ$ 下是封闭的，所以 $\circ(a_1, a_2, \cdots, a_n) \in S_1$。又因为 $a_1, a_2, \cdots, a_n \in S_2$，且 S_2 在运算 $\circ$ 下是封闭的，所以又有 $\circ(a_1, a_2, \cdots, a_n) \in S_2$。因此有 $\circ(a_1, a_2, \cdots, a_n) \in S_1 \cap S_2$。证完。

下面我们讨论二元运算的某些一般性质。

定义 4-3 设 $*$ 是集合 A 上的一个二元运算，如果对于任意的 $a, b \in A$，有 $a * b = b * a$，则称 $*$ 在 A 上是**可交换的**。

定义 4-4 设 $*$ 是集合 A 上的一个二元运算，如果对于任意的 $a, b, c \in A$，有 $a * (b * c) = (a * b) * c$，则称 $*$ 在 A 上是**可结合的**。

定义 4-5 设 $*$ 和 $\circ$ 是集合 A 上的二元运算，如果对于任意的 $a, b, c \in A$，有

$$a * (b \circ c) = (a * b) \circ (a * c);$$

$$(b \circ c) * a = (b * a) \circ (c * a),$$

则称 $*$ 对于 $\circ$ 是可分配的。

例如，实数集合 R 上的加和乘运算是可交换的，也是可结合的，但 R 上的减运算却是不可交换和不可结合的。乘对加是可分配的，但加对于乘是不可分配的。任一集合的幂集上的并和交运算是可交换和可结合的，而且并与交是相互可分配的。

若二元运算 $*$ 在 A 上是可结合的，则 $a*(b*c)=(a*b)*c$ 常记作没有括号的 $a*b*c$。

在前面各章我们曾多次提到把结合律推广到任意n个对象时，可用数学归纳法加以证明。现在我们就集合 A 上的二元运算给出其证明。

设 $*$ 是集合 A 上可结合的运算。要证明运算 $*$ 对任意 n 个元素 $a_1,a_2,\cdots,a_n$ 也是可结合的，只要证明在 $a_1*a_2*\cdots*a_n$ 中任意加括号所得的积(我们简称 A 中元素经 $*$ 运算的结果为积)等于按次序由左而右加括号所得的积

$$(\cdots(((a_1*a_2)*a_3)*a_4)\cdots a_{n-1})*a_n.$$

首先，当 $n=1$ 和 $n=2$ 时，上述命题显然成立。

当 $n=3$ 时，由结合律上述命题也成立。

其次，假设对少于n个元素的乘积上述命题成立，并设由$a_1*a_2*\cdots*a_n$ 任意加括号而得到的积为 α，设在 α 中最后一次计算是 β，γ 两部分相乘，即 $\alpha=(\beta)*(\gamma)$，因 γ 的元素个数小于 n，故由归纳假设，γ 等于按次序由左而右加括号所得的积$(\cdots)*a_n$。由结合律 $\alpha=(\beta)*(\gamma)=(\beta)*((\cdots)*a_n)=((\beta)*(\cdots))*a_n$， 而 $(\beta)*(\cdots)$ 的元素个数小于 n，故等于按次序由左而右加括号所得积

$$(\cdots((a_1*a_2)*a_3)\cdots a_{n-2})*a_{n-1},$$

因而 $\alpha=((\cdots((a_1*a_2)*a_3)\cdots a_{n-2})*a_{n-1})*a_n$。这就证明了对于 A 中任意 n 个元素运算 $*$ 都是可结合的。

于是，在这样的集合中，无括号的表达式 $a_1*a_2*\cdots*a_n$唯一地表示 A 中的一个元素。特别对于 $a*a*\cdots*a$(n 次)，我们记作 a^n，

并且称为 a 的 n 次幂，n 称为 a 的指数。形式的 a^n 还可归纳定义为：

$$a^1 = a,$$
$$a^{n+1} = a^n * a \qquad (n = 1, 2, 3, \cdots).$$

显然，如果运算 $*$ 是可结合的，则对任意的正整数 m 和 n，有

$$a^m * a^n = a^{m+n},$$
$$(a^m)^n = a^{mn}.$$

下面定义集合 A 中与二元运算相联系的一些特殊的元素。

定义 4-6 设 $*$ 是集合 A 上的二元运算，如果存在一个元素 $e_l \in A$，使得对于所有的 $a \in A$ 有 $e_l * a = a$，则称 e_l 是 A 上关于运算 $*$ 的**左单位元**；如果存在一个元素 $e_r \in A$，使得对于所有的 $a \in A$ 有 $a * e_r = a$，则称 e_r 是 A 上关于运算 $*$ 的**右单位元**；如果存在一个元素 $e \in A$，使得对于所有的 $a \in A$ 有 $e * a = a * e = a$，则称 e 是 A 上关于运算 $*$ 的**单位元**。

定理 4-2 设 $*$ 是集合 A 上的二元运算，又设 e_l 和 e_r 分别是 $*$ 的左单位元和右单位元，则 $e_l = e_r = e$，且 e 是 $*$ 的唯一的单位元。

证明 因 e_l 和 e_r 分别是 $*$ 的左、右单位元，所以 $e_l * e_r = e_r = e_l$。令 $e_l = e_r = e$，则 e 是 $*$ 的一个单位元。设 e' 也是 $*$ 的单位元，则 $e * e' = e = e'$，因此 e 是 $*$ 的唯一的单位元。证完。

定义 4-7 设 $*$ 是集合 A 上的二元运算，如果存在一个元素 $z_l \in A$，使得对于所有的 $a \in A$ 有 $z_l * a = z_l$，则称 z_l 是 A 上关于运算 $*$ 的**左零元**；如果存在一个元素 $z_r \in A$，使得对于所有的 $a \in A$ 有 $a * z_r = z_r$，则称 z_r 是 A 上关于运算 $*$ 的**右零元**；如果存在一个元素 $z \in A$，使得对于所有的 $a \in A$ 有 $z * a = a * z = z$，则称 z 是 A 上关于运算 $*$ 的**零元**。

类似于定理 4-2，我们有：

定理 4-3 设 $*$ 是集合 A 上的二元运算，又设 z_l 和 z_r 分别是 $*$ 的左零元和右零元，则 $z_l = z_r = z$，且 z 是 $*$ 的唯一的零元。

其证明与定理 4-2 的证明完全类似。

例如，对于实数集 R 上的加法运算来说，0 是其单位元，它没有零元。而乘法运算的单位元是 1，零元是 0。减法运算的右单位元是 0，它没有左单位元，因而也没有单位元。在幂集 2^U 上，ϕ 是集合并运算的单位元，交运算的零元；U 是交运算的单位元，并运算的零元。

定义 4-8 设 $*$ 是集合 A 上的二元运算。如果 $a*a=a$，则称元素 $a\in A$ 是 A 上关于运算 $*$ 的**幂等元**。

二元运算的单位元和零元都是幂等元。除了单位元和零元外，还可能有其它的幂等元。例如，每个集合都是并运算和交运算的幂等元。

定义 4-9 设 $*$ 是集合 A 上具有单位元 e 的二元运算，对于元素 $a\in A$，如果存在一元素 $a_l^{-1}\in A$，使得 $a_l^{-1}*a=e$，则称元素 a 对于运算 $*$ 是**左可逆的**，而称 a_l^{-1} 为 a 的**左逆元**；如果存在一元素 $a_r^{-1}\in A$，使得 $a*a_r^{-1}=e$，则称元素 a 关于运算 $*$ 是**右可逆的**，而称 a_r^{-1} 为 a 的**右逆元**；如果存在一元素 $a^{-1}\in A$，使得 $a^{-1}*a=a*a^{-1}=e$，则称 a 关于运算 $*$ 是**可逆的**，而称 a^{-1} 为 a 的**逆元**。

定理 4-4 设 $*$ 是集合 A 上具有单位元 e 且可结合的二元运算。如果元素 $a\in A$ 有左逆元和右逆元，则其左、右逆元相等，并且就是 a 的唯一的逆元。

证明 设 a_l^{-1} 和 a_r^{-1} 分别是 a 的左逆元和右逆元，则 $a_l^{-1}*a=a*a_r^{-1}=e$。因此

$$
\begin{aligned}
a_l^{-1}*a*a_r^{-1}&=(a_l^{-1}*a)*a_r^{-1}=e*a_r^{-1}=a_r^{-1}\\
&=a_l^{-1}*(a*a_r^{-1})=a_l^{-1}*e=a_l^{-1},
\end{aligned}
$$

于是 $a_l^{-1}=a_r^{-1}=a^{-1}$ 是 a 的一个逆元。

设 b 也是 a 的一个逆元，则

$$b=b*e=b*(a*a^{-1})=(b*a)*a^{-1}=e*a^{-1}=a^{-1}.$$

因此 a^{-1} 是 a 的唯一的逆元。证完。

由逆元的定义可知，如果 $a\in A$ 有逆元 a^{-1}，则有 $a*a^{-1}=a^{-1}*a=e$。因此 $(a^{-1})^{-1}=a$（即 a 是 a^{-1} 的逆元）。

显然，对于任何二元运算，单位元是可逆的，其逆元就是单位元自身，但一般零元不是可逆的。例如，每一个实数 $r\in R$ 都有一个关于加法运算的逆元 $-r$。每一个非零实数 $r\in R$，都有一个关于乘法运算的逆元 $\frac{1}{r}$，但数 0 不是可逆的。

二元运算的上述这些性质在代数系统中常被用来作为公理。

§4.2 代 数 系 统

一个非空集合和定义在该集合上的一个或多个运算所组成的系统称为一个**代数系统**，用记号 $\langle S; o_1, o_2, \cdots, o_n\rangle$ 表示，其中，S 是非空集合，称为这个代数系统的域；$o_1, o_2, \cdots, o_n$ 是 S 上的运算。注意，集合 S 上的各个运算可以是具有不同阶的运算。

代数系统 $\langle S; o_1, o_2, \cdots, o_n\rangle$ 的基数与 S 的基数意义相同，因此当 S 是有限集时，$\langle S; o_1, o_2, \cdots, o_n\rangle$ 称为**有限代数系统**。

例 1 设 R_A 表示集合 A 上所有关系的集合，$\cdot$ 是求复合关系的运算。显然 R_A 对运算 $\cdot$ 是封闭的，因此它们可以构成一个代数系统 $\langle R_A; \cdot\rangle$。其中 $\cdot$ 是 R_A 上的二元运算。

例 2 全集合 U 的幂集 2^U 对于集合的 $'$，$\cup$，$\cap$ 运算显然是封闭的，因此可构成代数系统 $\langle 2^U; ', \cup, \cap\rangle$，称之为**集合代数**。这里 $'$ 是 2^U 上的一元运算；$\cup$ 和 $\cap$ 是二元运算。

例 3 整数集 I 和定义在其上的通常的加法与乘法运算组成一个代数系统，记作 $\langle I; +, \cdot\rangle$，这两个运算都是 I 上的二元运算，具有如下的一些重要性质：

(1) 交换律　对任意的 i，$j\in I$，

$$i+j=j+i, \qquad i\cdot j=j\cdot i.$$

(2) 结合律　对任意的$i,j,k\in I$，

$$i+(j+k)=(i+j)+k, \qquad i\cdot(j\cdot k)=(i\cdot j)\cdot k.$$

(3) 分配律　对任意的$i,j,k\in I$，

$$i\cdot(j+k)=i\cdot j+i\cdot k.$$

(4) 单位元　I含有特殊的元素0和1，使得对于任意的$i\in I$，

$$i+0=0+i=i, \qquad 1\cdot i=i\cdot 1=i.$$

(5) 关于加法的可逆性　对于每一元素$i\in I$，都有一元素$-i\in I$，使得

$$(-i)+i=i+(-i)=0.$$

(6) 消去律　如果$i\neq 0$，则对任意的$j,k\in I$由$i\cdot j=i\cdot k$，可得$j=k$。

例4　实数集R和定义在其上的通常的加法和乘法运算组成代数系统$\langle R;+,\cdot\rangle$。容易验证$\langle R;+,\cdot\rangle$具有上述对于代数系统$\langle I;+,\cdot\rangle$所列出的全部性质。

例5　设有集合$B=\{a,b\}$和由下表给出的B上的运算$+$和$\cdot$：

$+$	a	b
a	a	b
b	b	a

$\cdot$	a	b
a	a	a
b	a	b

容易验证，代数系统$\langle B;+,\cdot\rangle$也具有对$\langle I;+,\cdot\rangle$所列出的全部性质。这里加法的单位元是a，乘法的单位元是b。

此外，有理数集Q和其上定义的通常的加法与乘法运算组成的代数系统$\langle Q;+,\cdot\rangle$也具有对$\langle I;+,\cdot\rangle$所列出的全部性质。

上述这些例子表明，不同的代数系统可能具有一些共同的性质。这一事实启发我们，不必一个一个地去研究各个代数系统，而是列出一组性质，把这一组性质看作是公理，我们研究满足这些公理的抽象的代数系统。在这样的抽象代数系统里，由这些公理推导出的任何有效的结论(定理)，对于满足这组公理的任何代数系统将都是成立的。为了作这样的讨论，我们将不考虑任何特

定的集合，也不给所具有的运算赋予任何特定的含义。这种系统的集合和运算仅仅是一些抽象的记号。而相应的代数系统就叫做抽象代数。

例如，我们可以将例 3 所列出的六条性质作为公理，定义一个称为“整环”的抽象的代数系统。

定义 4-10 设 J 是一个非空集合，$+$ 和 $\cdot$ 是 J 上的两个二元运算，如果运算 $+$ 和 $\cdot$ 满足前述性质(1)—(6)，则称代数系统 $\langle J; +, \cdot\rangle$ 为**整环**。

于是，代数系统 $\langle I; +, \cdot\rangle$、$\langle R; +, \cdot\rangle$、$\langle Q; +, \cdot\rangle$ 和 $\langle B; +, \cdot\rangle$ 都是整环。

定义 4-11 设 $\langle S; o_1, o_2, \cdots, o_n\rangle$ 是一个代数系统，$\tilde{S}$ 是 S 的一个非空子集，它在 S 的每一运算下都是封闭的，即对每一个 k_i 阶的运算 o_i 及对每一有序 k_i 元组 $(x_1, x_2, \cdots, x_{k_i}) \in \tilde{S}^{k_i}$，有 $o_i(x_1, x_2, \cdots, x_{k_i}) \in \tilde{S}$，则代数系统 $\langle \tilde{S}; \tilde{o}_1, \tilde{o}_2, \cdots, \tilde{o}_n\rangle$ 称为 $\langle S; o_1, o_2, \cdots, o_n\rangle$ 的**子系统**或**子代数**。其中运算 $\tilde{o}_i (i = 1, 2, \cdots, n)$ 是 k_i 阶的运算，对于每一 $(x_1, x_2, \cdots, x_{k_i}) \in \tilde{S}^{k_i}$，$\tilde{o}_i(x_1, x_2, \cdots, x_{k_i}) = o_i(x_1, x_2, \cdots, x_{k_i})$。

如上定义的运算 $\tilde{o}_i (i = 1, 2, \cdots, n)$ 是运算 o_i 在新域 $\tilde{S}$ 上的限制，因此为简便起见，$\langle \tilde{S}; \tilde{o}_1, \tilde{o}_2, \cdots, \tilde{o}_n\rangle$ 有时就记作 $\langle \tilde{S}; o_1, o_2, \cdots, o_n\rangle$。

若 $\tilde{S}$ 是 S 的真子集，则称 $\langle \tilde{S}; o_1, o_2, \cdots, o_n\rangle$ 是 $\langle S; o_1, o_2, \cdots, o_n\rangle$ 的**真子系统**或**真子代数**。

例 6 代数系统 $\langle E; +, \cdot\rangle$（这里 E 是所有偶数的集合，$+$ 和 $\cdot$ 是通常的加法和乘法）就是 $\langle I; +, \cdot\rangle$ 的子代数。若 M 表示所有奇数的集合，则 M 和运算 $+$，$\cdot$ 不能构成 $\langle I; +, \cdot\rangle$ 的子代数。

例 7 代数系统 $\langle [0, 1]; \cdot\rangle$（这里 $\cdot$ 是通常的乘法）是 $\langle R; \cdot\rangle$ 的子代数。

定义 4-12 设有两个代数系统 $V_1 = \langle S_1; o_{11}, o_{12}, \cdots, o_{1n}\rangle$，$V_2$

$=\langle S_2;o_{21},o_{22},\cdots,o_{2n}\rangle$，如果运算 o_{1i} 和 $o_{2i}(i=1,2,\cdots,n)$ 具有相同的阶，则称代数系统 V_1 和 V_2 是**同一类型的**。

§4.3 同态和同构

函数这个概念，对于代数系统来说，必须与代数系统中的运算发生联系，才能成为有力的工具。因此在讨论代数系统时，我们需要的是与运算有联系的函数。显然，元素运算的象等于这些元素的象的运算是一个重要的联系。本节就是讨论具有这种联系的重要函数。

定义 4-13 设 $V_1=\langle S_1;o_{11},o_{12},\cdots,o_{1n}\rangle$ 和 $V_2=\langle S_2;o_{21},o_{22},\cdots,o_{2n}\rangle$ 是两个同一类型的代数系统，即 o_{1i} 和 o_{2i} 都是 k_i 阶的运算 $(i=1,2,\cdots,n)$，h 是从 S_1 到 S_2 的一个函数，若对于每一个 k_i 元组 $(x_1,x_2,\cdots,x_{k_i})\in S_1^{k_i}$，有 $h(o_{1i}(x_1,x_2,\cdots,x_{k_i}))=o_{2i}(h(x_1),h(x_2),\cdots,h(x_{k_i}))$ $(i=1,2,\cdots,n)$，则称 h 是从代数系统 V_1 到 V_2 的一个**同态**（参见图4-1）。代数系统 V_2 常称为 V_1（在 h 下）的**同态象**。有时也说 h 将运算 o_{1i} 传送到运算 o_{2i} $(i=1,2,\cdots,n)$。

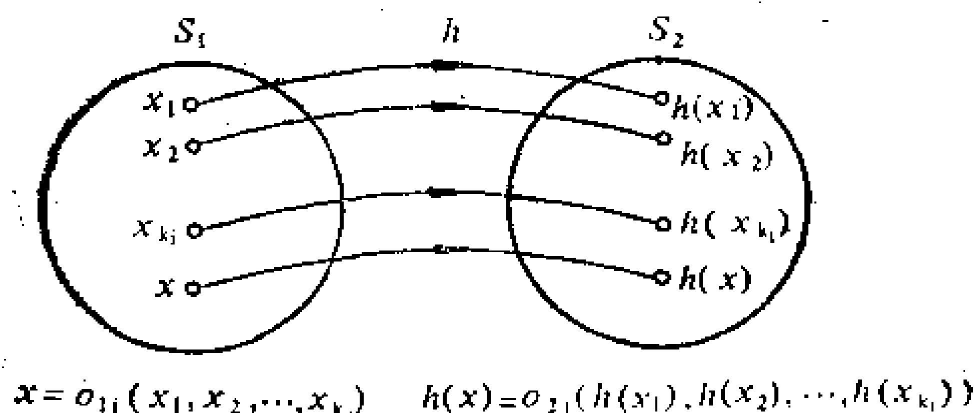


图 4-1

特别当 $n=2$，且运算都是二元运算时，上一定义也可以这样阐述：

设有代数系统 $V_1=\langle S_1;*,\Box\rangle$ 和 $V_2=\langle S_2;\bigstar,\cdot\rangle$，其中的运算都是二元运算，$h$ 是从 S_1 到 S_2 的函数，若对于所有的 $(x_1,x_2)\in S_1^2$，有

$$h(x_1*x_2)=h(x_1)\bigstar h(x_2);\quad h(x_1\Box x_2)=h(x_1)\cdot h(x_2),$$

则 h 是一个从 V_1 到 V_2 的同态（将 $*$ 传送到 $\bigstar$，将 $\Box$ 传送到 $\cdot$）。

由上看出，S_1 中任何两个元素 x_1 和 x_2 的“$*$积”的象，就是 x_1 和 x_2 在 S_2 上的象的“$\bigstar$积”。同样，x_1 和 x_2 的“$\Box$积”的象，就是 x_1 和 x_2 在 S_2 上的象的“$\cdot$积”。

例 1 考虑代数系统 $V_1=\langle I;+,\cdot\rangle$，其中 I 是整数集，$+$ 与 $\cdot$ 是通常的加法与乘法。并考虑代数系统 $V_2=\langle Z_6;\oplus_6,\odot_6\rangle$，其中 $Z_6=\{0,1,2,3,4,5\}$，而 $\oplus_6$（模 6 的加法）和 $\odot_6$（模 6 的乘法）定义为

$$z_1\oplus_6 z_2=\mathrm{res}_6(z_1+z_2),\qquad z_1\odot_6 z_2=\mathrm{res}_6(z_1\cdot z_2).$$

定义函数 h：$I\to Z_6$，对任意的 $i\in I$，有 $h(i)=\mathrm{res}_6(i)$，则 h 是一个从 V_1 到 V_2 的同态。这是因为对于所有的 $(i_1,i_2)\in I^2$，有

$$\mathrm{res}_6(i_1+i_2)=\mathrm{res}_6(i_1)\oplus_6\mathrm{res}_6(i_2),\tag{1}$$

$$\mathrm{res}_6(i_1\cdot i_2)=\mathrm{res}_6(i_1)\odot_6\mathrm{res}_6(i_2).\tag{2}$$

我们给出(1)式的证明：

设 $i_1=6q_1+r_1\quad(0\leqslant r_1<6)$，$i_2=6q_2+r_2\quad(0\leqslant r_2<6)$，

则 $$i_1+i_2=6(q_1+q_2)+(r_1+r_2),$$

所以 $$\mathrm{res}_6(i_1+i_2)=\mathrm{res}_6(r_1+r_2).$$

另一方面，$\mathrm{res}_6(i_1)\oplus_6\mathrm{res}_6(i_2)=r_1\oplus_6 r_2=\mathrm{res}_6(r_1+r_2)$，

因此 $$\mathrm{res}_6(i_1+i_2)=\mathrm{res}_6(i_1)\oplus_6\mathrm{res}_6(i_2).$$

对(2)式可类似地加以证明。

例 2 我们知道，整数集 I 上的“模 m 同余”关系是 I 上的等价关系。设 $m=4$，并令 $I_{(4)}$ 表示所生成的等价类集合，所以

$$I_{(4)}=\{[0],[1],[2],[3]\},$$

其中 $[i]$ 表示所有与 i 等价的那些整数的集合。我们定义 $I_{(4)}$ 上的

运算$\oplus$，对于任意的$[i],[j]\in I_{(4)}$，

$$[i]\oplus[j]=[\mathrm{res}_4(i+j)]。$$

运算$\oplus$描述在表4-2中，由于集合$I_{(4)}$对于运算$\oplus$是封闭的，因此可构成代数系统$\langle I_{(4)};\oplus\rangle$。

表4-2

$\oplus$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

考虑代数系统$\langle I_{(4)};\oplus\rangle$和$\langle B;+\rangle$。$\langle B;+\rangle$中的域$B$和运算$+$是§4.2例5中代数系统$\langle B;+,\cdot\rangle$的域$B$和运算$+$。

定义函数h：$I_{(4)}\to B$如下：

$h([0])=h([2])=a$，　　　$h([1])=h([3])=b$。

因为对任意的i，$j=0,1,2,3$，有

$$h([i]\oplus[j])=h([i])+h([j])，$$

所以h是一个由$\langle I_{(4)};\oplus\rangle$到$\langle B;+\rangle$的同态。

例3　给定代数系统$\langle I_{(4)};\oplus\rangle$和$\langle N;+\rangle$，定义函数$g$：$N\to I_{(4)}$如下：对任意的$n\in N$，

$$g(n)=[\mathrm{res}_4(n)]。$$

对任意的n，$m\in N$，令$g(n)=[i]$，$g(m)=[j]$，则

$$\begin{aligned}g(n+m)&=[\mathrm{res}_4(n+m)]=[\mathrm{res}_4(i+j)]=[i]\oplus[j]\\&=g(n)\oplus g(m)，\end{aligned}$$

因此，g是一个由$\langle N;+\rangle$到$\langle I_{(4)};\oplus\rangle$的同态。

不难看出，凡能满足定义4-13所给出的条件的函数，都是一个从V_1到V_2的同态。因此从一个代数系统到另一个代数系统，可能有多个同态映射。

根据函数是内射、满射和双射，我们可将相应的同态称为单一同态、满同态和同构。

定义 4-14 设 $h: S_1 \to S_2$ 是从 $V_1 = \langle S_1; o_{11}, o_{12}, \cdots, o_{1n} \rangle$ 到 $V_2 = \langle S_2; o_{21}, o_{22}, \cdots, o_{2n} \rangle$ 的同态。

(1) 如果 h 是内射，则称 h 是从 V_1 到 V_2 的**单一同态**。

(2) 如果 h 是满射，则称 h 是从 V_1 到 V_2 的**满同态**。

(3) 如果 h 是双射，则称 h 是从 V_1 到 V_2 的**同构**。

假设在定义 4-13 中两代数系统的运算 o_{11} 和 o_{21} 都是二元运算，那么如图4-2所示，所谓 h 将运算 o_{11} 传送到运算 o_{21}，即若 S_1 中任意两个元素 x_1 和 x_2，经 o_{11} 运算的结果为 x，则 x 在 S_2 中的象 $h(x)$ 恰好就是 x_1 和 x_2 在 S_2 中的象 $h(x_1)$ 和 $h(x_2)$ 经 o_{21} 运算的结果。也就是说，S_1 中元素之间由运算 o_{11} 所构成的关系，经 h 映射到 S_2 中后，其象之间的类似关系由 o_{21} 来构成，因此我们称同态是一个"保持运算"的映射。

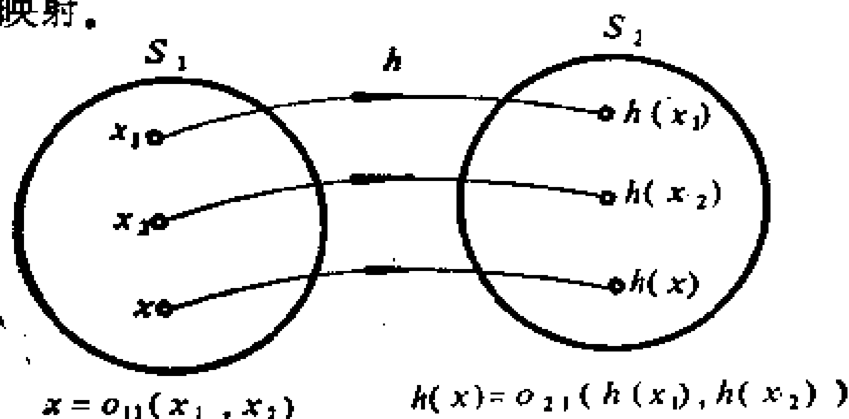


图 4-2

既然同态 h 能保持运算，那么我们不禁要问，同态能不能保持运算的性质呢？即运算 o_{11} 所具有的性质，运算 o_{21} 是否也具有呢？关于这，我们有下面的定理。

定理 4-5 设 $h: S_1 \to S_2$ 是从代数系统 $V_1 = \langle S_1; o_{11}, o_{12}, \cdots, o_{1n} \rangle$ 到代数系统 $V_2 = \langle S_2; o_{21}, o_{22}, \cdots, o_{2n} \rangle$ 的一个满同态，这里运算 o_{1i} 被传送到 o_{2i} $(i = 1, 2, \cdots, n)$。

(1) 若 o_{1i} 是一个二元可交换的运算，则 o_{2i} 也是一个二元可交换的运算；

(2) 若 o_{1i} 是一个二元可结合的运算，则 o_{2i} 也是一个二元可结合的运算；

(3) 若对于运算 o_{1i}，V_1 具有一单位元 e_i，则对于运算 o_{2i}，V_2 也具有单位元 $h(e_i)$；

(4) 若对于运算 o_{1i}，每一个元素 $x \in S_1$ 都有一个逆元 x^{-1}，则对于运算 o_{2i}，每一个元素 $h(x) \in S_2$ 都有一个逆元 $h(x^{-1})$，

(5) 若 o_{1i} 对于二元运算 o_{1j} 是可分配的，则 o_{2i} 对于 o_{2j} 也是可分配的。

证明 (1) 因为 h：$S_1 \to S_2$ 是一个满同态，所以它是一个满射。因而，S_2 中的每一个元素都可写成 $h(x)$ 的形式。这里 $x \in S_1$。如果 o_{1i} 是可交换的，则对于所有的 $h(x_1)$，$h(x_2) \in S_2$，有

$$o_{2i}(h(x_1), h(x_2)) = h(o_{1i}(x_1, x_2)) = h(o_{1i}(x_2, x_1))$$
$$= o_{2i}(h(x_2), h(x_1)),$$

这就证明了 o_{2i} 也是可交换的。

(3) 因为对于每一元素 $x \in S_1$，有 $o_{1i}(x, e_i) = o_{1i}(e_i, x) = x$，所以对于每一元素 $h(x) \in S_2$，有

$$o_{2i}(h(x), h(e_i)) = h(o_{1i}(x, e_i)) = h(o_{1i}(e_i, x))$$
$$= o_{2i}(h(e_i), h(x)),$$

又
$$o_{2i}(h(x), h(e_i)) = h(o_{1i}(x, e_i)) = h(x),$$

这就证明了对于运算 o_{2i}，V_2 有单位元 $h(e_i)$。

用类似的方法可证明定理中的其它结论。证完。

这个定理说明，与代数系统 V_1 相联系的一些重要公理，诸如交换律、结合律、分配律、同一律和可逆律，在 V_1 的任何满同态象中（特别在同构象中）能够被保持下来。此外，满同态 h：$S_1 \to S_2$ 还保持零元，即若对于运算 O_{1i}，V_1 具有一零元 z_i，则对于运算 O_{2i}，V_2 也具有零元 $h(z_i)$。其证明类似于定理 4-5(3)。

需要指出的是，若 $h: S_1 \to S_2$ 不是一个满同态，则定理 4-5 所列出的性质不一定成立。因为这时在 S_2 中存在有某些元素，它们不是 S_1 中任何元素的象。

如果 h 是一个从代数系统 V_1 到 V_2 的同构，那么 h 是从 S_1 到 S_2 的双射。由定理 3-4，h 的逆 h^{-1} 是一个由 S_2 到 S_1 的双射。而且，因为 S_2 中每一元素都是 h 作用下 S_1 中某一元素的象，所以 $S_2^{k_i}$ 中任一 k_i 元组 $(y_1, y_2, \cdots, y_{k_i})$ 可写为 $(h(x_1), h(x_2), \cdots, h(x_{k_i}))$ 的形式，并有

$$
\begin{aligned}
& h^{-1}[o_{2i}(h(x_1), h(x_2), \cdots, h(x_{k_i}))] \\
&= h^{-1}[h(o_{1i}(x_1, x_2, \cdots, x_{k_i}))] \\
&= (h^{-1}h)(o_{1i}(x_1, x_2, \cdots, x_{k_i})) = o_{1i}(x_1, x_2, \cdots, x_{k_i}) \\
&= o_{1i}[h^{-1}(h(x_1)), h^{-1}(h(x_2)), \cdots, h^{-1}(h(x_{k_i}))] \\
&\qquad\qquad (i = 1, 2, \cdots, n).
\end{aligned}
$$

这就是说，当 h 是从代数系统 V_1 到 V_2 的同构时，h 的逆函数 h^{-1} 是从 V_2 到 V_1 的同构。因此我们称 V_1 和 V_2 是彼此同构的。

由上述讨论可知，如果两个代数系统 $V_1 = \langle S_1; o_{11}, o_{12}, \cdots, o_{1n}\rangle$ 和 $V_2 = \langle S_2; o_{21}, o_{22}, \cdots, o_{2n}\rangle$ 彼此同构，则集合 S_1 中所有元素与集合 S_2 中所有元素一一对应，V_1 中的各运算与 V_2 中的各个运算一一对应。若 S_1 中元素之间有由运算 o_{1i} 所构成的关系时，则 S_2 中对应的元素之间也相应有由运算 o_{2i} 所构成的类似关系。反之亦然。因此，如果在 V_1 中有一个与运算 o_{1i} 有关的性质，则只要将 $x \in S_1$ 改为 $h(x) \in S_2$，运算 o_{1i} 改为 o_{2i}，在 V_2 中这个性质也同样成立。反之，如果在 V_2 中有一个与运算 o_{2i} 有关的性质，则只要将 $h(x) \in S_2$ 改为 $x \in S_1$，运算 o_{2i} 改为 o_{1i}，在 V_1 中这个性质也同样成立。所以两个同构的代数系统除了集合中元素的名字和运算的符号可能不同外，在本质上没有什么区别。研究 V_1 所导出的各种理论可直接应用于任一与 V_1 同构的

各代数系统中。于是在研究一个新的代数系统的性质时，确定这个代数系统与另一其性质已知的代数系统的同构，是十分重要的。

例 4 考虑代数系统 $V_1=\langle\{\phi,A,A',U\};\ ',\cup,\cap\rangle$，这里 A 是全集合 U 的一个固定的子集，而 $'$、$\cup$ 和 $\cap$ 是通常的集合运算。再考虑代数系统 $V_2=\langle\{1,2,5,10\};\sim,\vee,\wedge\rangle$，这里 $i_1\vee i_2$ 表示 i_1 和 i_2 的最小公倍数，$i_1\wedge i_2$ 表示 i_1 和 i_2 的最大公因数，而 $\tilde{i}$ 表示 10 除以 i 所得的商。于是 V_1 和 V_2 上的运算表如下：

S	S'
ϕ	U
A	A'
A'	A
U	ϕ

$\cup$	ϕ	A	A'	U
ϕ	ϕ	A	A'	U
A	A	A	U	U
A'	A'	U	A'	U
U	U	U	U	U

$\cap$	ϕ	A	A'	U
ϕ	ϕ	ϕ	ϕ	ϕ
A	ϕ	A	ϕ	A
A'	ϕ	ϕ	A'	A'
U	ϕ	A	A'	U

i	$\tilde{i}$
1	10
2	5
5	2
10	1

$\vee$	1	2	5	10
1	1	2	5	10
2	2	2	10	10
5	5	10	5	10
10	10	10	10	10

$\wedge$	1	2	5	10
1	1	1	1	1
2	1	2	1	2
5	1	1	5	5
10	1	2	5	10

显然，下面的三张表可由上面的三张表简单地分别用 1、2、5 和 10 代替 ϕ、A、A' 和 U，用 $\sim$、$\vee$ 和 $\wedge$ 分别代替 $'$、$\cup$ 和 $\cap$ 而得到。所以 V_1 和 V_2 同构。由于有同构 $h:\{\phi,A,A',U\}\to\{1,2,5,10\}$，这里 $h(\phi)=1$，$h(A)=2$，$h(A')=5$，$h(U)=10$，因此对 V_1 所导出的任何性质，简单地作上述替换后可直接用于 V_2。

例 5 设 E 是偶数的集合，$E=\{\cdots,-4,-2,0,2,4,\cdots\}$，则代数系统 $\langle I;+\rangle$ 和 $\langle E;+\rangle$ 是同构的。因为存在函数 $f: I\to E$ 使得 $f(i)=2i$，显然 f 是一个双射，而且对于任意的整数 i 和

j，有

$$f(i+j)=2(i+j)=2i+2j=f(i)+f(j).$$

例 6 代数系统 $\langle Z; +\rangle$ 和 $\langle N; \cdot\rangle$ 不是同构的。对于这一结论，我们可用反证法加以证明。假设 h 是从 $\langle Z; +\rangle$ 到 $\langle N; \cdot\rangle$ 的一个同构，在 N 里有无穷多个素数。因为 h 是从 Z 到 N 的满射，因此必存在某个 $x\in Z(x\geqslant 3)$ 和某个素数 $p\in N(p\geqslant 2)$，使得 $h(x)=p$，由于 h 是一个同构，因此有

$$p=h(x)=h(x+0)=h(x)\cdot h(0),$$

$$p=h(x)=h((x-1)+1)=h(x-1)\cdot h(1).$$

而 p 是一个素数，p 的因子仅是 p 和 1，所以有 $h(0)=1$，且有 $h(x-1)=1$ 或 $h(1)=1$，但 $0<1<x-1<x$，故在映射 h 之下 1 至少是两个元素的象，这与 h 是双射矛盾。因此，从 $\langle Z; +\rangle$ 到 $\langle N; \cdot\rangle$ 不存在同构。

显然，每一个代数系统对其自身是同构的。又如果 V_1 对 V_2 是同构的，则 V_2 对 V_1 也是同构的。而且如果 V_1 对 V_2 是同构的，V_2 对 V_3 是同构的，则 V_1 对 V_3 也是同构的。因此，在由代数系统所组成的集合上同构关系是一个等价关系。我们可将这个集合分划成一些等价类。其中每一类是由具有相同“结构”的同构代数系统所组成。

若 V_1 和 V_2 是同一代数系统 V，则从 V_1 到 V_2 的同态称为 V 的**自同态**；从 V_1 到 V_2 的同构称为**自同构**。

§4.4 同余关系

定义 4-15 设有代数系统 $V=\langle S; o_1, o_2, \cdots, o_n\rangle$，其中所有的 o_i 都是一元运算。ρ 是 S 上的一个等价关系。若对于所有的 $x, y\in S$，由 $x\rho y$，可得 $(o_i(x)\rho(o_i(y))$，则称 ρ 对于运算 o_i 满足**代换性质**。若 ρ 对于所有的运算 $o_i\ (i=1,2,\cdots,n)$ 都满足代换性

质，则称 ρ 为 V 上的一个**同余关系**。

例 1　设有代数系统 $\langle I; o\rangle$，这里 o 是一个一元运算，定义为 $o(i)=\text{res}_m(i^2)$（m 为某一正整数）。设 ρ 是 I 上的一个关系，定义为：当且仅当 $\text{res}_m(i_1)=\text{res}_m(i_2)$ 时，有 $i_1\rho i_2$。由 §2.6 例 2，ρ 是一个等价关系。现在设 i_1，$i_2\in I$ 且满足 $i_1\rho i_2$，于是 $\text{res}_m(i_1)=\text{res}_m(i_2)$。我们将 i_1 和 i_2 分别写成 $i_1=q_1m+r$ 和 $i_2=q_2m+r$，这里 $0\leqslant r<m$，从而

$$o(i_1)=\text{res}_m(i_1^2)=\text{res}_m((q_1m+r)^2)=\text{res}_m(q_1^2m^2+2q_1mr+r^2)$$
$$=\text{res}_m(r^2);$$
$$o(i_2)=\text{res}_m(i_2^2)=\text{res}_m((q_2m+r)^2)=\text{res}_m(q_2^2m^2+2q_2mr+r^2)$$
$$=\text{res}_m(r^2).$$

因此有 $o(i_1)=o(i_2)$。当然有 $(o(i_1))\rho(o(i_2))$。所以 ρ 是 $\langle I; o\rangle$ 上的同余关系。

下面我们将要说明，同余关系的概念和同态的概念有着密切的联系。此外，借助于同余关系，可以由一个给定的代数系统构造出新的更简单的代数系统。

定理 4-6　设 h 是一个从代数系统 $V=\langle S; o_1,o_2,\cdots,o_n\rangle$ 到代数系统 $V^*=\langle S^*; o_1^*,o_2^*,\cdots,o_n^*\rangle$ 的同态，其中所有的 o_i 都是一元运算，$o_i^*(i=1,2,\cdots,n)$ 是 o_i 经 h 传送到的运算。在 S 上定义一个关系 ρ_h，使得当且仅当 $h(x_1)=h(x_2)$ 时，$x_1\rho_h x_2$，则 ρ_h 是 V 上的同余关系。

上述关系 ρ_h 在 §3.5 中曾被称为 h 的等价核。

证明　显然，ρ_h 是 S 上的一个等价关系。现在设 $x_1\rho_h x_2$，则 $h(x_1)=h(x_2)$，因此有

$$o_i^*(h(x_1))=o_i^*(h(x_2))\qquad (i=1,2,\cdots,n),$$

又因为 h 是一个同态，所以有

$$h(o_i(x_1))=h(o_i(x_2)),$$

因而 $$(o_i(x_1))\rho(o_i(x_2))\qquad (i=1,2,\cdots,n),$$

即 ρ_k 对于所有运算 o_i 满足代换性质。故 ρ_k 是 V 上的同余关系。证完。

在§2.6 中我们曾介绍过商集的概念。所谓集合 A 关于 ρ 的商集，是指当在给定集合 A 上定义了一个等价关系 ρ 时，ρ 可导致 A 上一等价分划 $\pi_\rho^A=\{[a]_\rho|a\in A\}$，这个分划，即所有等价类的集合，就叫做集合 A 关于 ρ 的商集，用 A/ρ 来表示。

相应地，若在某代数系统 V 上定义了一个同余关系 ρ，则我们也可定义一个新的代数系统，并且称它为代数系统 V 关于 ρ 的商代数。

定义 4-16 设有代数系统 $V=\langle S; o_1,o_2,\cdots,o_n\rangle$，其中所有的 o_i 都是一元运算，ρ 是 V 上的一个同余关系。构造一个新的代数系统 $\tilde{V}=\langle\tilde{S};\tilde{o}_1,\tilde{o}_2,\cdots,\tilde{o}_n\rangle$，

其中
$$\tilde{S}=S/\rho=\{[x]_\rho|x\in S\},\tag{4-1}$$
即 $\tilde{S}$ 是集合 S 关于 ρ 的商集。

每一个运算 $\tilde{o}_i$ 都是由下式定义的一元运算：
$$\tilde{o}_i([x]_\rho)=[o_i(x)]_\rho\qquad(i=1,2,\cdots,n).\tag{4-2}$$
则新的代数系统 $\tilde{V}$ 称为 V 关于 ρ 的**商代数**，表示为 V/ρ。

为了说明上面所定义的系统确实是一个代数系统，我们必须证明所有运算 $\tilde{o}_i$ 是有定义的，也就是要证明应用 $\tilde{o}_i$ 运算（$i=1,2,\cdots,n$）的结果不依赖于表示等价类所使用的元素。

事实上，若 $[x]_\rho=[y]_\rho$，则有 $x\rho y$。由于 ρ 是一个同余关系，因此对于所有的运算 o_i，有 $(o_i(x))\rho(o_i(y))$，从而有 $[o_i(x)]_\rho=[o_i(y)]_\rho$。而 $\tilde{o}_i([x]_\rho)=[o_i(x)]_\rho$，$\tilde{o}_i([y]_\rho)=[o_i(y)]_\rho$。于是得 $\tilde{o}_i([x]_\rho)=\tilde{o}_i([y]_\rho)$，因此所有运算 $\tilde{o}_i$ 都是有定义的。

关于商代数有如下两个性质：

定理 4-7 设 $V=\langle S; o_1, o_2,\cdots, o_n\rangle$ 是一个代数系统，其中所有的运算 o_i 都是一元运算，ρ 是 V 上的一个同余关系，则存在一个从 V 到 V/ρ 的满同态。

证明 定义函数 h：$S \to \tilde{S}$，使得对任意的 $x \in S$，$h(x) = [x]_\rho$。因为每一个 $[x]_\rho$ 非空，所以必有某一元素 x，使得 $h(x) = [x]_\rho$，因而 h 是一个满射。又对于每一个运算 o_i，$h(o_i(x)) = [o_i(x)]_\rho = \tilde{o}_i([x]_\rho) = \tilde{o}_i(h(x))$。所以 h 是一个从 V 到 V/ρ 的满同态。证完。

上述两定理说明了同态与同余关系的密切联系，即对于任何一个从代数系统 V 到 V^* 的同态 h，可以定义一个 V 上的同余关系；而对于代数系统 V 上的任何一个同余关系 ρ，可以定义一个从 V 到 V 关于 ρ 的商代数的一个满同态。

定理 4-8 设 h 是一个从 $V = \langle S; o_1, o_2, \cdots, o_n \rangle$ 到 $V^* = \langle S^*; o_1^*, o_2^*, \cdots, o_n^* \rangle$ 的满同态，其中所有的运算 o_i 都是一元运算，$o_i^*(i = 1, 2, \cdots, n)$ 是 o_i 经 h 传送到的运算，ρ_h 是 h 的等价核。则 V^* 和 V/ρ_h 是同构的。

证明 因为 h 是同态，根据定理 4-6，ρ_h 是 V 上的同余关系。因此可按（4-1）式和（4-2）式来构造商代数 $V/\rho_h = \langle \tilde{S}; \tilde{o}_1, \tilde{o}_2, \cdots, \tilde{o}_n \rangle$。

因为 h 是一个从 S 到 S^* 的满射，所以对于每个 $x^* \in S^*$，必存在某个 $x \in S$，使得 $x^* = h(x)$。现定义函数 f：$S^* \to S/\rho_h$，使得 $f(h(x)) = [x]_{\rho_h}$（参见图 4-3）。

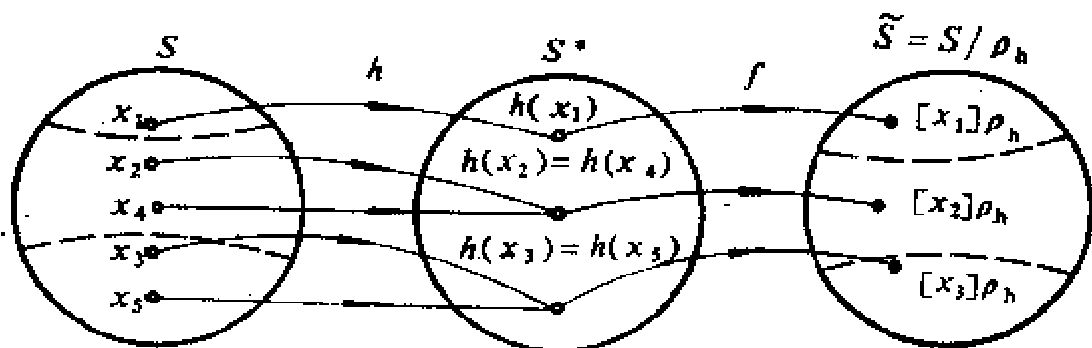


图 4-3

f 是一个满射，因为对于每一个 $[x]_{\rho_h}$，必有一个 $h(x)$，使得 $f(h(x)) = [x]_{\rho_h}$。

f 是一个内射，因为如果 $[x]_{\rho_h} = [y]_{\rho_h}$，则 $x\rho_h y$，由 ρ_h 的定义有 $h(x) = h(y)$。

因此 f 是一个双射。

又因为 h 是一个同态，所以对于每一个运算 o_i^*，有

$$f(o_i^*(h(x))) = f(h(o_i(x))) = [o_i(x)]_{\rho_h} = \tilde{o}_i([x]_{\rho_h})$$
$$= \tilde{o}_i(f(h(x)))。$$

所以 V^* 和 V/ρ_h 是同构的。证完。

例 2 设有代数系统 $V = \langle I; ' \rangle$（这里 I 是整数集，而 $i' = i + 1$）和代数系统 $V^* = \langle B; * \rangle$〔这里 $B = \{0, 1\}$，而 $b^* = \text{res}_2(b + 1)$。（即 $0^* = 1, 1^* = 0$）〕。定义满射 h：$I \to B$，使得 $h(i) = \text{res}_2(i)$。由于

$$h(i') = h(i + 1) = \text{res}_2(i + 1) = \text{res}_2(\text{res}_2(i) + 1) = (\text{res}_2(i))^*$$
$$= (h(i))^*,$$

因此 h 是一个从 V 到 V^* 的满同态。

现在在 I 上定义关系 ρ_h。当且仅当 $h(i_1) = h(i_2)$ 时，即当且仅当 $\text{res}_2(i_1) = \text{res}_2(i_2)$ 时，$i_1\rho_h i_2$，显然 ρ_h 是一个等价关系。又若 $i_1\rho_h i_2$，则 $\text{res}_2(i_1) = \text{res}_2(i_2)$，作与前面类似的推导，我们有

$$h(i_1') = (\text{res}_2(i_1))^*, \qquad h(i_2') = (\text{res}_2(i_2))^*,$$

因而有
$$h(i_1') = h(i_2'),$$

于是 $i_1'\rho_h i_2'$（根据定理 4-6，ρ_h 的确是一个同余关系）。

ρ_h 在 I 上导出的等价分划是 $\pi^I_{\rho_h} = \{[0], [1]\}$，$V$ 关于 ρ_h 的商代数是 $\tilde{V} = \langle \tilde{I}; ☆ \rangle$，其中

$$\tilde{I} = I/\rho_h = \{[0], [1]\}，而 [i]^☆ = [i'] \ (i = 0, 1)。$$

定义函数 f：$B \to \tilde{I}$，使得 $f(b) = [b]$。显然，f 是一个双射，又 $f(b^*) = [b^*] = [\text{res}_2(b + 1)]$，

$$(f(b))^☆ = ([b])^☆ = [b'] = [b + 1] = [\text{res}_2(b + 1)],$$

所以 $f(b^*)=(f(b))^*$，因此 f 是一个从 V^* 到 $\tilde{V}$ 的同构（根据定理 4-14 也知 V^* 和 $\tilde{V}$ 是同构的）。

上述同余关系是定义在所有运算都是一元运算的代数系统上。同余关系的概念也可推广到具有任意阶运算的代数系统上。推广的关键是推广等价关系 ρ 对于任意 k_i 阶运算（k_i 是正整数）的代换性质。

定义 4-17 设有代数系统 $V=\langle S; o_1, o_2, \cdots, o_n\rangle$，其中 o_i ($i=1,2,\cdots,n$) 是任意阶（假设为 k_i 阶）的运算，ρ 是 S 上的一个等价关系。若对于任意的 k_i 元组 $(x_1, x_2, \cdots, x_{k_i})$，$(x_1', x_2', \cdots, x_{k_i}')\in S^{k_i}$，

由
$$x_1\rho x_1', x_2\rho x_2', \cdots, x_{k_i}\rho x_{k_i}',$$
可推得
$$(o_i(x_1, x_2, \cdots, x_{k_i}))\rho(o_i(x_1', x_2', \cdots, x_{k_i}')),$$
则称 ρ 对于 k_i 阶运算 o_i 满足代换性质。若 ρ 对于所有运算 o_i ($i=1,2,\cdots,n$) 都满足代换性质，则称 ρ 是 V 上的一个**同余关系**。

根据推广的同余关系的定义，可以证明，对于任一代数系统 $\langle S; o_1, o_2, \cdots, o_n\rangle$ 定理 4-6、4-7、4-8 仍都成立，而对于运算 o_i 的阶没有任何限制。

首先，对于任意代数系统 $V=\langle S; o_1, o_2, \cdots, o_n\rangle$ 可仿照前述的方法定义 V 关于同余关系 ρ 的**商代数**
$$V/\rho=\langle\tilde{S}; \tilde{o}_1, \tilde{o}_2, \cdots, \tilde{o}_n\rangle,$$
其中
$$\tilde{S}=S/\rho=\{[x]_\rho \mid x\in S\},$$
所有运算 $\tilde{o}_i$ 定义为
$$\tilde{o}_i([x_1]_\rho, [x_2]_\rho, \cdots, [x_{k_i}]_\rho)=[o_i(x_1, x_2, \cdots, x_{k_i})]_\rho \quad (i=1,2,\cdots,n).$$
这样定义的运算 $\tilde{o}_i$ 与 o_i 同阶，其运算结果不依赖于表示等价类所使用的元素，因而是有定义的。

对于任意代数系统，定理 4-6、4-7、4-8 可叙述为如下形式。

定理 4-9 对于任一代数系统 $V=\langle S; o_1, o_2, \cdots, o_n\rangle$，

(1) 若 h 是一个从代数系统 V 到代数系统 $V^* = \langle S^*; o_1^*, o_2^*, \cdots, o_m^* \rangle$ 的同态，则 h 的等价核 ρ_h 是 V 上的一个同余关系；

(2) 若 ρ 是 V 上的一个同余关系，则存在一个从 V 到 V/ρ 的满同态；

(3) 若 h 是一个从 V 到 V^* 的满同态，而 ρ_h 是 h 的等价核，则 V^* 与 V/ρ_h 是同构的。

这些结论的证明都不难，只要对一元的情况作简单的修改即可给出。现以 (1) 为例给出其证明，其它可仿照给出。

证明 显然，ρ_h 是 S 上的一个等价关系。设 $(x_1, x_2, \cdots, x_{k_i})$，$(x_1', x_2', \cdots, x_{k_i}') \in S^{k_i}$，且有

$$x_1 \rho_h x_1', \ x_2 \rho_h x_2', \cdots, x_{k_i} \rho_h x_{k_i}',$$

因此有 $\quad h(x_1) = h(x_1'),\ h(x_2) = h(x_2'), \cdots, h(x_{k_i}) = h(x_{k_i}'),$

从而有 $\quad o_i^*(h(x_1), h(x_2), \cdots, h(x_{k_i}))$

$$= o_i^*(h(x_1'), h(x_2'), \cdots, h(x_{k_i}')).$$

又因为 h 是一个同态，所以有

$$h(o_i(x_1, x_2, \cdots, x_{k_i})) = h(o_i(x_1', x_2', \cdots, x_{k_i}')),$$

即 $\quad (o_i(x_1, x_2, \cdots, x_{k_i})) \rho_h (o_i(x_1', x_2', \cdots, x_{k_i}')),$

于是，ρ_h 对于运算 o_i 满足代换性质。由于 o_i 的任意性，故 ρ_h 是 V 上的同余关系。证完。

例 3 设有代数系统 $V = \langle N; + \rangle$，其中 $+$ 是通常的加法运算，在 N 上定义一个关系 ρ，使得当且仅当 $x_1 - x_2$ 能被 4 整除时，$x_1 \rho x_2$（即"模 4 同余"关系）。显然 ρ 是一个等价关系。此外，ρ 还是一个同余关系。因为对于任意 $x_1 \rho x_1'$，$x_2 \rho x_2'$，有 $4 \mid x_1 - x_1'$，$4 \mid x_2 - x_2'$，所以 $(x_1 + x_2) - (x_1' + x_2') = (x_1 - x_1') + (x_2 - x_2')$ 也能被 4 整除，于是 $(x_1 + x_2) \rho (x_1' + x_2')$。

V 关于 ρ 的商代数 $V/\rho = \langle \widetilde{N}, \oplus \rangle$，其中

$$\widetilde{N} = N/\rho = \{[1]_\rho, [2]_\rho, [3]_\rho, [4]_\rho\};$$

$$[i_1]_\rho \oplus [i_2]_\rho = [i_1 + i_2]_\rho.$$

定义函数 f：$N \to \hat{N}$，使得 $f(x)=[x]_\rho$，则 f 是由 V 到 V/ρ 的满同态。因为，显然 f 是一个满射，又对于任意的 x_1，$x_2 \in N$，

$$f(x_1+x_2)=[x_1+x_2]_\rho=[x_1]_\rho \oplus [x_2]_\rho = f(x_1)\oplus f(x_2).$$

（根据定理 4-9(2) 也可知 f 是一个由 V 到 V/ρ 的满同态）

定义 4-18 设 $V=\langle S;*\rangle$ 是一个代数系统，这里 $*$ 是一个二元运算。若对于任意的 $x_1,x_2,x_3 \in S$，

由 $x_1\rho x_2$，　　可得 $(x_1*x_3)\rho(x_2*x_3)$，

则称 S 上的等价关系 ρ 为 V 上的一个**右同余关系**。若对于任意的 $x_1,x_2,x_3 \in S$，

由 $x_1\rho x_2$，　　可得 $(x_3*x_1)\rho(x_3*x_2)$，

则称 S 上的等价关系 ρ 为 V 上的一个**左同余关系**。

定理 4-10 若 ρ 在 $V=\langle S;*\rangle$ 上既是右同余关系，又是左同余关系，则 ρ 是 V 上的一个同余关系。

证明 对于任意的 x_1,x_2,x_3，$x_4 \in S$，若 $x_1\rho x_2$，$x_3\rho x_4$，则由 ρ 既是右同余，又是左同余，可得

$$(x_1*x_3)\rho(x_2*x_3),\quad (x_2*x_3)\rho(x_2*x_4).$$

又由于 ρ 是等价关系，故由 ρ 的可传递性，有

$$(x_1*x_3)\rho(x_2*x_4).$$

所以 ρ 是 V 上的一个同余关系。证完。

§4.5 积代数

在上一节里，我们介绍了借助于同余关系由一个给定的代数系统构造出另一个新的代数系统的方法。本节我们再介绍借助于集合的笛卡尔积由有限个给定的同类型的代数系统构造出一个新的代数系统的方法。

定义 4-19 设有代数系统

$$
\left.\begin{aligned}
V_1 &= \langle S_1; o_{11}, o_{12}, \cdots, o_{1n}\rangle; \\
V_2 &= \langle S_2; o_{21}, o_{22}, \cdots, o_{2n}\rangle; \\
&\vdots \\
V_r &= \langle S_r; o_{r1}, o_{r2}, \cdots, o_{rn}\rangle,
\end{aligned}\right\} \tag{4-3}
$$

其中，$o_{1i}, o_{2i}, \cdots, o_{ri}$ $(i=1,2,\cdots,n)$ 是同为 k_i 阶的运算，$V_1, V_2, \cdots, V_r$ 的**积代数**或**直积**是代数系统

$$
V = \langle S; o_1, o_2, \cdots, o_n\rangle, \tag{4-4}
$$

其中，$S = S_1 \times S_2 \times \cdots \times S_r = \{(x_1, x_2, \cdots, x_r) \mid x_i \in S_i, i = 1, 2, \cdots, n\}$；$o_i$ $(i=1,2,\cdots,n)$ 是 k_i 阶的运算，其定义如下：对于任意 k_i 个元素 $(x_1^{(1)}, x_2^{(1)}, \cdots, x_r^{(1)})$，$(x_1^{(2)}, x_2^{(2)}, \cdots, x_r^{(2)})$，$\cdots$，$(x_1^{(k_i)}, x_2^{(k_i)}, \cdots, x_r^{(k_i)}) \in S$，

$$
\begin{aligned}
& o_i((x_1^{(1)}, x_2^{(1)}, \cdots, x_r^{(1)}), (x_1^{(2)}, x_2^{(2)}, \cdots, x_r^{(2)}), \cdots, \\
& (x_1^{(k_i)}, x_2^{(k_i)}, \cdots, x_r^{(k_i)})) \\
& \quad = (o_{1i}(x_1^{(1)}, x_1^{(2)}, \cdots, x_1^{(k_i)}), o_{2i}(x_2^{(1)}, x_2^{(2)}, \cdots, x_2^{(k_i)}), \cdots, \\
& \qquad o_{ri}(x_r^{(1)}, x_r^{(2)}, \cdots, x_r^{(k_i)}))。
\end{aligned}
$$

V 一般表示为 $V_1 \times V_2 \times \cdots \times V_r$。

例 1 代数系统 $V_1 = \langle A; *\rangle = \langle\{a_1, a_2\}; *\rangle$，

$$V_2 = \langle B; \circ\rangle = \langle\{b_1, b_2, b_3\}; \circ\rangle,$$

其中，$*$ 和 $\circ$ 都是二元运算，由表 4-3 给出。

表 4-3

$*$	a_1	a_2
a_1	a_1	a_2
a_2	a_2	a_1

$\circ$	b_1	b_2	b_3
b_1	b_1	b_1	b_3
b_2	b_2	b_2	b_3
b_3	b_1	b_3	b_3

V_1 和 V_2 的积代数是代数系统

$$V_1 \times V_2 = \langle A \times B; \square\rangle,$$

其中，$A\times B=\{(a_1,b_1),(a_1,b_2),(a_1,b_3),(a_2,b_1),(a_2,b_2),(a_2,b_3)\}$。对于任意的 $(a_i,b_j),(a_k,b_l)\in A\times B$，有

$$(a_i,b_j)\,\square\,(a_k,b_l)=(a_i*a_k,b_j\circ b_l).$$

例如 $(a_1,b_2)\,\square\,(a_2,b_1)=(a_1*a_2,b_2\circ b_1)=(a_2,b_2)$；

$(a_2,b_1)\,\square\,(a_1,b_2)=(a_2*a_1,b_1\circ b_2)=(a_2,b_1)$。

表 4-4 给出了□的运算表。

表 4-4

□	(a_1,b_1)	(a_1,b_2)	(a_1,b_3)	(a_2,b_1)	(a_2,b_2)	(a_2,b_3)
(a_1,b_1)	(a_1,b_1)	(a_1,b_1)	(a_1,b_3)	(a_2,b_1)	(a_2,b_1)	(a_2,b_3)
(a_1,b_2)	(a_1,b_2)	(a_1,b_2)	(a_1,b_3)	(a_2,b_2)	(a_2,b_2)	(a_2,b_3)
(a_1,b_3)	(a_1,b_1)	(a_1,b_3)	(a_1,b_3)	(a_2,b_1)	(a_2,b_3)	(a_2,b_3)
(a_2,b_1)	(a_2,b_1)	(a_2,b_1)	(a_2,b_3)	(a_1,b_1)	(a_1,b_1)	(a_1,b_3)
(a_2,b_2)	(a_2,b_2)	(a_2,b_2)	(a_2,b_3)	(a_1,b_2)	(a_1,b_2)	(a_1,b_3)
(a_2,b_3)	(a_2,b_1)	(a_2,b_3)	(a_2,b_3)	(a_1,b_1)	(a_1,b_3)	(a_1,b_3)

定理 4-11 设 $V_1,V_2,\cdots,V_r$ 和 V 是 (4-3) 式和 (4-4) 式中所定义的代数系统，其中 $o_{j1}(j=1,2,\cdots,r)$ 是二元运算，

(1) 若 $o_{j1}(j=1,2,\cdots,r)$ 是可交换的运算，则 o_1 也是可交换的运算；

(2) 若 $o_{j1}(j=1,2,\cdots,r)$ 是可结合的运算，则 o_1 也是可结合的运算；

(3) 若对于运算 o_{j1}，V_j 有单位元 $e_j(j=1,2,\cdots,r)$，则 V 对于 o_1 有单位元 $(e_1,e_2,\cdots,e_r)$；

(4) 若每一元素 $x_j\in S_j$ 对于 $o_{j1}(j=1,2,\cdots,r)$ 有逆元 x_j^{-1}，则每一元素 $(x_1,x_2,\cdots,x_r)\in S$ 对于 o_1 有逆元 $(x_1^{-1},x_2^{-1},\cdots,x_r^{-1})$；

(5) 若 o_{j1} 对二元运算 $o_{j2}(j=1,2,\cdots,r)$ 是可分配的，则 o_1 对 o_2 也是可分配的。

证明 (1) 若 $o_{j1}(j=1,2,\cdots,r)$ 是可交换的，则对于所有的 $(x_1,x_2,\cdots,x_r)$，$(x_1',x_2',\cdots,x_r')\in S$，

$$\begin{aligned}
&o_1((x_1,x_2,\cdots,x_r),(x_1',x_2',\cdots,x_r'))\\
&=(o_{11}(x_1,x_1'),o_{21}(x_2,x_2'),\cdots,o_{r1}(x_r,x_r'))\\
&=(o_{11}(x_1',x_1),o_{21}(x_2',x_2),\cdots,o_{r1}(x_r',x_r))\\
&=o_1((x_1',x_2',\cdots,x_r'),(x_1,x_2,\cdots,x_r)),
\end{aligned}$$

即 o_1 也是可交换的。

(3) 若 $e_1,e_2,\cdots,e_r$ 分别是 $V_1,V_2,\cdots,V_r$ 对于运算 $o_{11},o_{21},\cdots,o_{r1}$ 的单位元，则对于所有的 $(x_1,x_2,\cdots,x_r)\in S$，

$$\begin{aligned}
&o_1((x_1,x_2,\cdots,x_r),(e_1,e_2,\cdots,e_r))\\
&=(o_{11}(x_1,e_1),o_{21}(x_2,e_2),\cdots,o_{r1}(x_r,e_r))\\
&=(x_1,x_2,\cdots,x_r),
\end{aligned}$$

同样地 $o_1((e_1,e_2,\cdots,e_r),(x_1,x_2,\cdots,x_r))=(x_1,x_2,\cdots,x_r)$，即 $(e_1,e_2,\cdots,e_r)$ 是 V 对于运算 o_1 的单位元。

其它结论的证明类似。证完。

注意，由于代数系统中运算符号的排列次序是任意的，因此定理 4-11 不仅对于运算 o_1 成立，而且对于所有运算 $o_i(i=1,2,\cdots,n)$ 都成立。

定理 4-11 说明，与代数系统相联系的某些重要公理(如交换律、结合律、分配律、同一律和可逆律)在这些系统的积代数中被保持。

习　题

1. 在下列N的子集中，哪些在加法下是封闭的？证明你的回答。

(1) $\{n|n$的某一次幂可被16整除$\}$；

(2) $\{n|n$与5互素$\}$；

(3) $\{n|6$整除n，而24整除$n^2\}$；

(4) $\{n|9$整除$21n\}$。

2. 证明在减法下封闭的整数的集合在加法下一定也是封闭的。

3. 下面是实数集合R上的二元运算$*$的不同定义。在每一情况下，判定$*$是否是可交换的，是否是可结合的，R对于$*$是否有单位元？如果有单位元的话，R中的每一元素对于$*$是否都是可逆的？

(1) $r_1 * r_2 = |r_1 - r_2|$；　　(2) $r_1 * r_2 = (r_1^2 + r_2^2)^{1/2}$；

(3) $r_1 * r_2 = r_1 + 2r_2$；　　(4) $r_1 * r_2 = \frac{1}{2}(r_1 + r_2)$。

4. 根据运算表怎样识别一个可交换的二元运算？怎样识别单位元和逆元(如果存在的话)？

5. 列举几个你所熟悉的代数系统。

6. $\langle A; *\rangle$是一个代数系统，这里$*$是可结合的二元运算，并且对于所有的$a_i, a_j \in A$，由$a_i * a_j = a_j * a_i$，可推得$a_i = a_j$。试证明对于任意的$a \in A$，$a * a = a$。

7. 若$\langle J; +, \cdot\rangle$是一整环，证明：

(1) 对所有的$i, j, k \in J$，若$i + j = i + k$，则$j = k$；

(2) 对所有的$i, j \in J$，方程$i + x = j$在J上有唯一解；

(3) 对所有的$i \in J$，$i \cdot 0 = 0 \cdot i = 0$；

(4) 对所有的 $i, j \in J$，若 $i \cdot j = 0$，则 $i = 0$ 或 $j = 0$；

(5) 对所有的 $i \in J$，$-(-i) = i$；

(6) 对所有的 $i \in J$，$-(i) = (-1) \cdot i$；

(7) 对所有 $i, j \in J$，$-(i+j) = (-i) + (-j)$；

(8) 对所有 $i, j \in J$，$(-i) \cdot j = i \cdot (-j) = -(ij)$；

(9) 对所有 $i, j \in J$，$(-i) \cdot (-j) = i \cdot j$.

8. 证明 $\langle C; +, \cdot \rangle$ 是一整环，其中，C 是复数的集合，而 + 和 · 是复数的加法和乘法。

9. $\langle \{2i | i \in I\}; +, \cdot \rangle$（此处 + 和 · 是通常的加法和乘法）是整环吗？

10. 设有代数系统 $\langle N; \cdot \rangle$ 和 $\langle \{0, 1\}; \cdot \rangle$，这里 · 是通常的乘法. 证明函数 $h: N \to \{0, 1\}$ 是一个从 $\langle N; \cdot \rangle$ 到 $\langle \{0, 1\}; \cdot \rangle$ 的同态，这里

$$h(n) = \begin{cases} 1 & n = 2^k (k \geq 0); \\ 0 & \text{否则}. \end{cases}$$

11 下表定义了代数系统 $\langle \{a, b, c, d\}; * \rangle$ 和 $\langle \{\alpha, \beta, \gamma, \delta\}; \cdot \rangle$，证明这两个代数系统同构。

*	a	b	c	d
a	d	a	b	d
b	d	b	c	d
c	a	d	c	c
d	a	b	a	a

·	α	β	γ	δ
α	β	β	β	δ
β	α	α	δ	β
γ	γ	β	γ	α
δ	α	α	γ	δ

12. 考虑代数系统 $\langle C; +, \cdot \rangle$（这里 C 是复数集合，+ 和 · 是复数的加法和乘法）和代数系统 $\langle H; +, \cdot \rangle$（这里 H 是所有形如

$$\begin{bmatrix} r_1 & r_2 \\ -r_2 & r_1 \end{bmatrix} \quad (r_1, r_2 \in R)$$

的 2×2 矩阵的集合，+ 和 · 是矩阵的加法和乘法），证明这两个代数系统同构。

13. 代数系统 $\langle\{0,1\};+,\cdot\rangle$（这里+和·表示布尔加法和乘法）与代数系统 $\langle\{-1,1\};\vee,\wedge\rangle$（这里 $i\vee j$ 和 $i\wedge j$ 分别表示元素 i 和 j 的最大者和最小者）是同构的吗？证明你的回答。

14. 完成定理4-5的证明。

15. 设 $f: X\to Y$ 是从 $V_1=\langle X;\circ\rangle$ 到 $V_2=\langle Y;*\rangle$ 的同态，$g: Y\to Z$ 是从 V_2 到 $V_3=\langle Z;\times\rangle$ 的同态，其中运算∘、∗和×都是二元运算。试证明：$gf: X\to Z$ 是从 V_1 到 V_3 的同态。

16. 设函数 $h: S_1\to S_2$ 是从代数系统 $V_1=\langle S_1;o_{11},o_{12},\cdots,o_{1n}\rangle$ 到 $V_2=\langle S_2;o_{21},o_{22},\cdots,o_{2n}\rangle$ 的同态。试证明 $\langle h(S_1);o_{21},o_{22},\cdots,o_{2n}\rangle$ 是 V_2 的子代数。

17. 考虑代数系统 $\langle I;\circ\rangle$（这里∘是一元运算，定义为 $\circ(i)=\text{res}_m(i^k)\ (m>0,k>0)$）。$I$ 上的关系 ρ 定义为：当且仅当 $\text{res}_m(i_1)=\text{res}_m(i_2)$ 时，$i_1\rho i_2$。ρ 是 $\langle I;\circ\rangle$ 上的同余关系吗？

18. 考虑代数系统 $\langle I;+,\cdot\rangle$（其中+和·是通常的加法和乘法）和关系 ρ（这里，当且仅当 $|i_1|=|i_2|$ 时，$i_1\rho i_2$）。ρ 对于+满足代换性质吗？对于·呢？

19. 代数系统 $V=\langle A;o_1,o_2\rangle$，这里 $A=\{a_1,a_2,a_3,a_4,a_5\}$，运算 o_1 和 o_2 由下表定义：

a_i	$o_1(a_i)$	$o_2(a_i)$
a_1	a_4	a_3
a_2	a_5	a_2
a_3	a_4	a_1
a_4	a_2	a_3
a_5	a_1	a_5

A 上的等价关系 ρ 产生 A 的分划 $\{\{a_1,a_3\},\{a_2,a_5\},\{a_4\}\}$。证明 ρ 是 V 上的同余关系。确定商代数 V/ρ（通过构造它的运算表）和从 V 到 V/ρ 上的满同态。

20. 证明集合A上的恒等关系I_A和普遍关系U_A都是$\langle A; o_1, o_2, \cdots, o_n\rangle$上的同余关系。这里$o_i$都是一元运算。

21. 完成定理4-9的证明。

22. 考虑代数系统$V=\langle Z_3; \oplus_3, \odot_3\rangle$和$Z_3$上的等价关系$\rho$。

(1) 证明若ρ对于$\oplus_3$满足代换性质，则它对$\odot_3$一定也满足代换性质。

(2) 找出一个Z_3上的等价关系，它对于$\odot_3$满足代换性质，但对$\ominus_3$不满足。

23. 完成定理4-11证明。

24. 代数系统$V_1=\langle Z_2; \oplus_2, \odot_2\rangle$和$V_2=\langle Z_3; \oplus_3, \odot_3\rangle$，构造$V_1\times V_2$和$V_2\times V_1$的运算表。

25. 给定代数系统$V_1=\langle Z_2; \oplus_2\rangle$，$V_2=\langle Z_3; \oplus_3\rangle$和$V_3=\langle Z_6; \oplus_6\rangle$。

(1) 证明$V_1\times V_2$同构于V_3；

(2) 给出$V_1\times V_2$上的所有同余关系。

第五章　群

上一章我们介绍了一般代数系统的概念，并举出了一些代数系统的例子。从这一章开始，我们将进入抽象代数系统的研究。

本章讨论具有一个二元运算的抽象代数系统，这样的代数系统常称为二元代数。我们从最简单的二元代数半群开始，然后研究独异点，最后研究在理论上和应用上都十分重要的二元代数——群。在介绍群的基本性质后，引入子群和陪集的概念。

对于计算机科学工作者来说，掌握群的知识是重要的。因为对于代码的查错、纠错的研究、自动机理论等各个方面的研究，群是其基础。

§5.1　半群和独异点

定义 5-1　设 S 是一个非空集合，$*$ 是 S 上的一个二元运算，如果运算 $*$ 是可结合的，则称代数系统 $\langle S; *\rangle$ 为**半群**。

例 1　代数系统 $\langle N; \cdot\rangle$ 和 $\langle N; +\rangle$ 都是半群。其中 $\cdot$ 和 $+$ 分别表示通常的乘法和加法。

例 2　仍用 $\cdot$ 表示通常的乘法运算，则代数系统 $\langle [0,1]; \cdot\rangle$ 和 $\langle (0,1); \cdot\rangle$ 也都是半群。

例 3　代数系统 $\langle I; +\rangle$ 和 $\langle R_+; \cdot\rangle$ 是半群，但代数系统 $\langle I; -\rangle$ 和 $\langle R_+; /\rangle$ 不是半群。其中 R_+ 表示所有正实数的集合，$+$、$-$、$\cdot$、$/$ 是通常的四则运算。

一个半群对于它的运算 $*$，可以有单位元，也可以没有单位元。

定义 5-2 若半群$\langle S; *\rangle$对于运算$*$有单位元，则称该半群为**独异点**。

在§4.1中我们已证明了，对于任意二元运算的单位元，如果它存在，则它是唯一的。因此独异点具有唯一的单位元。

例 4 $\langle Z; \cdot\rangle$和$\langle Z; +\rangle$都是独异点。其中$\cdot$和$+$是通常的乘法和加法运算。其单位元分别是数1和0。例1中的$\langle N; \cdot\rangle$是独异点，因为它具有单位元1。但$\langle N; +\rangle$不是独异点。

例 5 代数系统$\langle 2^U; \cup\rangle$和$\langle 2^U; \cap\rangle$分别是以ϕ和U为单位元的独异点。

例 6 设S是一个非空集合，$P(S)$是S的所有分划的集合。定义集合$P(S)$上的二元运算$*$，使得对于任意的$\pi_1, \pi_2 \in P(S)$，$\pi_1 * \pi_2$是由π_1的每个元素与π_2的每个元素的交集所组成的集合，其中去掉空集。

例如，若$S = \{a, b, c, d, e, f\}$，

$$\pi_1 = \{\{a, b\}, \{c\}, \{d, e, f\}\},$$

$$\pi_2 = \{\{a, b, c\}, \{d\}, \{e, f\}\},$$

则$\pi_1 * \pi_2 = \{\{a, b\}, \{c\}, \{d\}, \{e, f\}\}$。

容易证明，集合$P(S)$对于运算$*$是封闭的，即对任意的$\pi_1, \pi_2 \in P(S)$，$\pi_1 * \pi_2$仍是集合S的一个分划。且由$*$的定义可知，$*$是可结合的，分划$\pi = \{S\}$是运算$*$的单位元，因此$\langle P(S); *\rangle$是一个独异点。

定义 5-3 如果独异点$\langle S; *\rangle$中的运算$*$是可交换的，则称独异点$\langle S; *\rangle$是**可交换的独异点**。

我们已遇到过许多可交换的独异点。例如，$\langle 2^U; \cup\rangle$和$\langle 2^U; \cap\rangle$，$\langle Z; \cdot\rangle$和$\langle Z; +\rangle$以及$\langle P(S); *\rangle$都是可交换的独异点。

例 7 设R_A表示集合A上所有关系的集合，$\cdot$表示求复合关系的运算，则代数系统$\langle R_A; \cdot\rangle$是一个独异点。恒等关系$I_A$是其单位元。由于关系的复合不满足交换律，故$\langle R_A; \cdot\rangle$不是可交换的

独异点。

例 8 设 $V=\{a,b,c,\cdots,z\}$。这样的集合 V 称做字母表。其中的元素叫做字母、字符或符号。由字母表 V 中有限个字母组成的任何行，称为字母表 V 上的句子或行。由 m 个字母（$m\geqslant 0$）组成的行称为长度为 m 的行。例如：ab，ba，aa，bb 都是长度为 2 的行，aba，abb 是长度为 3 的行。空行是不包含任何字母的行，通常用 ε 表示。字母表 V 上所有行的集合用 V^* 表示。而非空行的集合用 $V^+=V^*-\{\varepsilon\}$ 表示。

定义 V^* 上的一个二元运算 $\circ$，对于任意的 $\alpha,\beta\in V^*$，$\alpha\circ\beta$ 是把行 α 写在行 β 的左边而得到的行。即 $\alpha\circ\beta=\alpha\beta$。显然，$\alpha\circ\beta\in V^*$。因此 V^* 对于运算 $\circ$ 是封闭的。V^* 上的这一运算 $\circ$，称为**链接**。例如行 $abaab$ 和行 bb 的链接就产生 $abaabbb$。容易看出，链接是可结合的。因此 $\langle V^*;\circ\rangle$ 是一个半群。又因为对于任意的行 $\alpha\in V^*$，有 $\alpha\circ\varepsilon=\varepsilon\circ\alpha=\alpha$。即 ε 是链接运算的单位元。所以 $\langle V^*;\circ\rangle$ 是一个独异点。但运算 $\circ$ 是不可交换的，所以 $\langle V^*;\circ\rangle$ 是一个不可交换的独异点。

在具有单位元 e 的独异点 $\langle S;*\rangle$ 中，元素 a 的幂可如下归纳地定义为：

$$a^0=e,$$

$$a^{n+1}=a^n*a,\qquad (n=0,1,2,\cdots).$$

不难证明，对于任意非负整数 m 和 n，我们有

$$a^m*a^n=a^{m+n},\qquad (a^m)^n=a^{mn}.$$

定义 5-4 在独异点 $\langle S;*\rangle$ 中，如果存在一个元素 $g\in S$，使得每一元素 $a\in S$ 都能写成 g^i（$i\geqslant 0$）的形式，则称独异点 $\langle S;*\rangle$ 为**循环独异点**，元素 g 称为该循环独异点的**生成元**。

定理 5-1 每一个循环独异点都是可交换的。

证明 设 $\langle S;*\rangle$ 是一具有生成元 g 的循环独异点，则对于任意的 $a,b\in S$，必存在整数 m，$n\geqslant 0$，使得 $a=g^m$，$b=g^n$，因此

$$a*b=g^m*g^n=g^{m+n}=g^n*g^m=b*a.\qquad \text{证完。}$$

例 9 $\langle Z;+\rangle$ 是一循环独异点，它的单位元是 0，生成元是 1。

例 10 设 $\langle S;*\rangle$ 是一个独异点，其中 $S=\{1, a, b, c, d\}$，表 5-1 给出了运算 $*$ 的定义。

表 5-1

*	1	a	b	c	d
1	1	a	b	c	d
a	a	a	b	d	d
b	b	b	d	a	a
c	c	d	a	b	b
d	d	d	a	b	b

显然 1 是单位元。因而有 $1=c^0$，又 $c=c^1$，$b=c*c=c^2$，$a=b*c=c^2*c=c^3$，$d=a*c=c^3*c=c^4$。

所以 $\langle S;*\rangle$ 是一循环独异点，其生成元是 c。

设 $\langle S;*\rangle$ 是具有单位元 e 和生成元 g 的一有限循环独异点。考虑无限序列 $e, g, g^2, g^3, \cdots$，此序列必然包含 S 的所有元素，而且，由于 S 只有有限个元素，因此必存在这样的正整数 n，它使得 g^n 是在序列中已经出现过的元素。设 n 是一个这样的最小的正整数，使得 $g^n=g^m(m<n)$，则此序列可以写成如下形式：

$$e, g, g^2, \cdots, g^m, g^{m+1}, \cdots, g^{n-1}, g^m, g^{m+1}, \cdots, g^{n-1}, g^m, g^{m+1}, \cdots, g^{n-1}, \cdots$$

从而 S 恰好具有 n 个元素，即

$$S=\{e, g, g^2, \cdots, g^{n-1}\}.$$

设 $n-m=l$，则对于任意的 $i\geqslant m$，有 $g^i=g^{i+hl}$（h 是任意的非负整数）。我们取 $i=kl$，这里 kl 是使得 $kl\geqslant m$ 的 l 的最小倍数，取 $h=k$，则有

$$g^{kl}=g^{kl+kl}=g^{kl}*g^{kl}.$$

因此，g^{kl} 是一幂等元。当 $m\neq 0$ 时，$g^{kl}\neq e$，所以 S 至少含有一个

除 e 以外的幂等元。

定理 5-2 设 $\langle S;*\rangle$ 是一有限独异点，则对每一 $a\in S$，存在一个整数 $j\geqslant 1$，使得 a^j 是一幂等元。

证明 对任一元素 $a\in S$，考虑二元代数 $\langle S_a;*\rangle$，这里 $S_a=\{e, a, a^2, a^3, \cdots\}$。显然，$\langle S_a;*\rangle$ 是一具有生成元 a 的有限循环独异点，因此至少有一幂等元 a^{kl}。这里的 k 和 l 如前所定义。证完。

例 10 中，由于 $c^5=c*d=b=c^2$，因此 $m=2, n=5, l=5-2=3$。故对于任意的 $i\geqslant 2$，有 $c^{i+3h}=c^i\ (h\geqslant 0)$。特别 $c^{3+3}=c^3$。因此 $c^3=a$ 是幂等元（实际上，从表 5-1，我们有 $a^2=a$）。

为了说明定理 5-2，考虑独异点 $\langle\{1, d, d^2, d^3, \cdots\};*\rangle$，因为

$$d^1=d,\ d^2=b,\ d^3=a,\ d^4=d,$$

所以对于任意的 $i\geqslant 1$，我们有 $d^{i+3h}=d^i$，特别 $d^{3+3}=d^3$，因此 d^3 是幂等元。

将子代数的概念应用到半群和独异点上，可得到子半群和子独异点的概念。

定义 5-5 设 $\langle S;*\rangle$ 是一个半群，如果 $\langle T;*\rangle$ 是 $\langle S;*\rangle$ 的子代数，则称 $\langle T;*\rangle$ 是 $\langle S;*\rangle$ 的**子半群**。

子半群也是一个半群。因为运算 $*$ 在 S 上是可结合的，当限制在 T 上时，它当然也是可结合的。

对任意的 $a\in S$，令 $T=\{a, a^2, a^3, \cdots\}$。则 $\langle T;*\rangle$ 是 $\langle S;*\rangle$ 的一个子半群。

定义 5-6 设 $\langle S;*\rangle$ 是一个独异点，$\langle T;*\rangle$ 是 $\langle S;*\rangle$ 的子代数，且单位元 $e\in T$，则称 $\langle T;*\rangle$ 是 $\langle S;*\rangle$ 的**子独异点**。

与子半群一样，子独异点也是一个独异点。

例 11 对半群 $\langle N;\cdot\rangle$（其中 $\cdot$ 是通常的乘法），设 $N_e=\{2n\mid n\in N\}$，由于 $\langle N_e;\cdot\rangle$ 是 $\langle N;\cdot\rangle$ 的子代数，因而是 $\langle N;\cdot\rangle$ 的子半群。

例 12 设有独异点 $\langle S;*\rangle$，其中 $S=\{e, 0, 1\}$，运算 $*$ 由下表定义。

*	e	0	1
e	e	0	1
0	0	0	0
1	1	0	1

$\langle S;*\rangle$ 的子代数 $\langle\{0,1\};*\rangle$ 是 $\langle S;*\rangle$ 的子半群。虽然它是一个独异点（1 是其单位元），但它不是 $\langle S;*\rangle$ 的子独异点。因为单位元 $e\notin\{0,1\}$。

$\langle\{e,0\};*\rangle$ 是 $\langle S;*\rangle$ 的子独异点。

例 13 $\langle R;+\rangle$ 是一独异点。数 0 是其单位元（其中 + 是通常的加法运算）。显然，$\langle I;+\rangle$ 和 $\langle Z;+\rangle$ 都是 $\langle R;+\rangle$ 的子独异点。

定理 5-3 设 $\langle S;*\rangle$ 是一个可交换的独异点，则 S 的所有幂等元的集合形成 $\langle S;*\rangle$ 的一个子独异点。

证明 设 T 是 S 中所有幂等元的集合。因为单位元 e 是幂等的，所以 $e\in T$。又设 $a,b\in T$，则有 $a*a=a$，$b*b=b$，因而由 $*$ 的可交换性，

$$(a*b)*(a*b)=(a*a)*(b*b)=a*b,$$

即 $a*b\in T$。故 $\langle T;*\rangle$ 是 $\langle S;*\rangle$ 的一个子独异点。证完。

代数系统的同态（包括单一同态、满同态）、同构和积代数的概念以及一些有关的结论，对于半群和独异点来说都是适用的。而且，由于半群和独异点都是十分简单的代数系统，因此把这些概念和结论应用于半群和独异点是一件很容易的事，这里不再赘述。需要指出的是利用满同态的关系可以判定某些代数系统是半群或独异点。

定理 5-4 设 h 是从代数系统 $V_1=\langle S_1;*\rangle$ 到 $V_2=\langle S_2;\circ\rangle$ 的满同态。其中运算 $*$ 和 $\circ$ 都是二元运算，则

(1) 若 V_1 是半群，则 V_2 也是半群；

(2) 若 V_1 是独异点，则 V_2 也是独异点。

证明 (1) 因为$V_1=\langle S_1;*\rangle$是半群，所以运算$*$是可结合的，而h是从V_1到V_2的满同态，由定理4-5可知，运算$\circ$也是可结合的。所以$V_2=\langle S_2;\circ\rangle$也是一个半群。

(2) 的证明可类似地给出。证完。

§5.2 群的定义

定义 5-7 设$\langle G;*\rangle$是一个代数系统。如果G上的二元运算$*$满足下列三个条件，则称$\langle G;*\rangle$是一个**群**。

(1) 对任意的$a,b,c\in G$，

$$a*(b*c)=(a*b)*c_{\circ}$$

(2) 存在一元素$e\in G$，使得对所有的$a\in G$，

$$e*a=a*e=a_{\circ}$$

(3) 对每一个$a\in G$，存在一个元素$a^{-1}\in G$，使得

$$a^{-1}*a=a*a^{-1}=e.$$

定义 5-8 如果群$\langle G;*\rangle$的运算$*$是可交换的，则称该群为**交换群**或**阿贝尔群**(N. H. Abel. 1802—1829挪威数学家)。

例 1 二元代数$\langle I;+\rangle$是一个群，这里运算$+$是通常的加法，其单位元是0，每一个整数i的逆元是$-i$。由于加法运算是可交换的，因此$\langle I;+\rangle$是一个阿贝尔群。

例 2 二元代数$\langle Q-\{0\};\cdot\rangle$，其中$\cdot$是通常的乘法，是一个阿贝尔群。其单位元是1，每一个有理数q的逆元是$\frac{1}{q}$。

例 3 独异点$\langle Z;+\rangle$和$\langle I;\cdot\rangle$都不是群。因为在$\langle Z;+\rangle$中每一个正整数都没有逆元。在$\langle I;\cdot\rangle$中除±1以外，每一元素都没有逆元。

例 4 集合$A=\{a,b,c\}$上的所有置换的集合$P=\{1,\alpha,\beta,\gamma,\delta,\varepsilon\}$，其中

$$1=\begin{pmatrix}a&b&c\\a&b&c\end{pmatrix},\quad \alpha=\begin{pmatrix}a&b&c\\a&c&b\end{pmatrix},\quad \beta=\begin{pmatrix}a&b&c\\b&a&c\end{pmatrix},$$

$$\gamma=\begin{pmatrix}a & b & c\\ b & c & a\end{pmatrix},\quad \delta=\begin{pmatrix}a & b & c\\ c & a & b\end{pmatrix},\quad \varepsilon=\begin{pmatrix}a & b & c\\ c & b & a\end{pmatrix}.$$

由于集合 A 上置换的集合对于置换的复合运算是封闭的，因此我们可以定义代数系统 $\langle P;\circ\rangle$，其中运算 $\circ$ 表示集合 A 上置换的复合运算。p 和 q 的复合 $p\circ q(p,q\in P)$ 是表示置换 p 后再接着置换 q 所产生的一种置换。

例如 $\beta\circ\delta=\begin{pmatrix}a & b & c\\ b & a & c\end{pmatrix}\begin{pmatrix}a & b & c\\ c & a & b\end{pmatrix}=\begin{pmatrix}a & b & c\\ a & c & b\end{pmatrix}=\alpha.$

运算 $\circ$ 的运算表列在表 5-2 中。

置换的复合就是函数的复合。因此 $\circ$ 是可结合的。显然，恒等置换 1 是其单位元。每一个置换都有逆置换，即逆元（$1^{-1}=1$，$\alpha^{-1}=\alpha$，$\beta^{-1}=\beta$，$\gamma^{-1}=\delta$，$\delta^{-1}=\gamma$，$\varepsilon^{-1}=\varepsilon$）。因此 $\langle P;\circ\rangle$ 是一个群。由运算表关于主对角线不是对称的这一事实可知，$\langle P;\circ\rangle$ 不是阿贝尔群。

事实上，任一 $\#A=n(n\in N)$ 的集合 A 上的所有（$n!$ 个）n 次置换的集合，对于置换的复合运算总是构成一个群。这种群叫做 **n 次对称群**，n 次对称群的任何子群叫做（n 次）**置换群**。例如，$\langle P;\circ\rangle$ 是一个 3 次置换群。$\langle\{1,\gamma,\delta\};\circ\rangle$，$\langle\{1,\alpha\};\circ\rangle$，$\langle\{1,\beta\};\circ\rangle$，$\langle\{1,\varepsilon\};\circ\rangle$ 也都是 3 次置换群。由于每一有限群与一个置换群同构，因此抽象群的研究可以转化为置换群的研究。

表 5-2

$\circ$	1	α	β	γ	δ	ε
1	1	α	β	γ	δ	ε
α	α	1	γ	β	ε	δ
β	β	δ	1	ε	α	γ
γ	γ	ε	α	δ	1	β
δ	δ	β	ε	1	γ	α
ε	ε	γ	δ	α	β	1

例 5 图5-1给出了一个用四元组(A,B,C,D)表示其角的正方形，可以用各种方法使该正方形转动，作变成它自己的刚性运动，而这些角表示四元组(A,B,C,D)的各种重新排列。

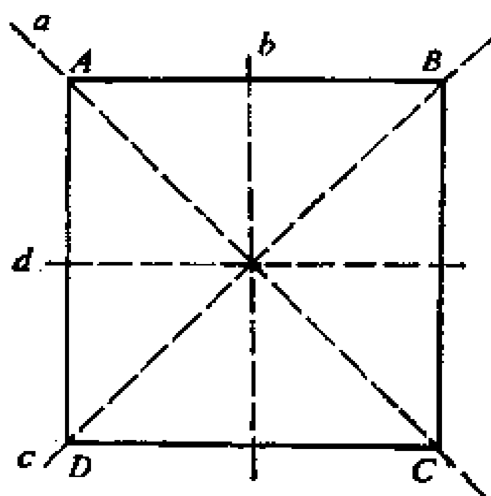


图 5-1

这样的刚性运动共有 8 个，每一个都可以用四个顶点的置换表示出来：

$$1=\begin{pmatrix}A&B&C&D\\A&B&C&D\end{pmatrix}\quad\text{(同一变换)},$$

$$\alpha_1=\begin{pmatrix}A&B&C&D\\D&A&B&C\end{pmatrix}\quad\text{(顺时针方向旋转90°)},$$

$$\alpha_2=\begin{pmatrix}A&B&C&D\\C&D&A&B\end{pmatrix}\quad\text{(顺时针方向旋转180°)},$$

$$\alpha_3=\begin{pmatrix}A&B&C&D\\B&C&D&A\end{pmatrix}\quad\text{(顺时针方向旋转270°)},$$

$$\alpha_4=\begin{pmatrix}A&B&C&D\\A&D&C&B\end{pmatrix}\quad\text{(绕直线 }a\text{ 翻转180°)},$$

$$\alpha_5=\begin{pmatrix}A&B&C&D\\B&A&D&C\end{pmatrix}\quad\text{(绕直线 }b\text{ 翻转180°)},$$

$$\alpha_6=\begin{pmatrix}A&B&C&D\\C&B&A&D\end{pmatrix}\quad\text{(绕直线 }c\text{ 翻转180°)},$$

$$\alpha_7=\begin{pmatrix}A&B&C&D\\D&C&B&A\end{pmatrix}\quad\text{(绕直线 }d\text{ 翻转180°)}.$$

虽然集合 $\{A,B,C,D\}$ 上可能的置换的数目是 $4!=24$，然而借助于正方形的刚性运动，可能得到的所有置换仅上面的 8 种。表5-3定义了集合 $P=\{1,\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5,\alpha_6,\alpha_7\}$ 上的二元运算 $\cdot$，例如 $\alpha_6\cdot\alpha_3$ 就是置换 α_6 将 (A,B,C,D) 变换成为 (C,B,A,D)，继而用 α_3 将 (C,B,A,D) 变换成为 (D,C,B,A)，因此 $\alpha_6\cdot\alpha_3=\alpha_7$。

表 5-3

$\cdot$	1	α_1	α_2	α_3	α_4	α_5	α_6	α_7
1	1	α_1	α_2	α_3	α_4	α_5	α_6	α_7
α_1	α_1	α_2	α_3	1	α_5	α_6	α_7	α_4
α_2	α_2	α_3	1	α_1	α_6	α_7	α_4	α_5
α_3	α_3	1	α_1	α_2	α_7	α_4	α_5	α_6
α_4	α_4	α_7	α_6	α_5	1	α_3	α_2	α_1
α_5	α_5	α_4	α_7	α_6	α_1	1	α_3	α_2
α_6	α_6	α_5	α_4	α_7	α_2	α_1	1	α_3
α_7	α_7	α_6	α_5	α_4	α_3	α_2	α_1	1

由表 5-3 可看出，P 对于运算 $\cdot$ 是封闭的。而运算 $\cdot$ 是可结合的，有单位元 1，P 中每一个元素都可逆，这些也是显而易见的。因此 $\langle P;\cdot\rangle$ 是一个群（该群称为这正方形的对称性群）。

在独异点中，我们定义了元素的非负整数次幂，即

$$a^0=e,\quad a^{n+1}=a^n*a,\quad (n=0,1,2,\cdots).$$

现在我们再定义 $\quad a^{-n}=(a^{-1})^n,\quad (n=1,2,3,\cdots).$

容易验证，对于任意的整数 m 和 n（正、负或零），下面二式仍然成立：

$$a^m*a^n=a^{m+n},\qquad (a^m)^n=a^{mn}.$$

因此又有

$$a^{-n}=(a^n)^{-1}.$$

定义 5-9 在群 $\langle G;*\rangle$ 中，如果存在一个元素 $g\in G$，使得每一元素 $a\in G$ 都能写成 $g^i\ (i\in I)$ 的形式，则称群 $\langle G;*\rangle$ 为**循环群**。而 g 称为该循环群的**生成元**，并说群 $\langle G;*\rangle$ 由 g 生成。

例6 群$\langle I;+\rangle$是一个循环群，其生成元是1。因为由定义单位元$0=1^0$，又任一正整数$n=\underbrace{1+1+\cdots+1}_{n\text{个}}$，任一负整数$-n=\underbrace{(-1)+(-1)+\cdots+(-1)}_{n\text{个}}$。

由定理5-1，每一循环群必是阿贝尔群。

定义5-10 设$\langle G;*\rangle$是一个群，如果G是有限集，则称$\langle G;*\rangle$是一**有限群**。G中元素的个数称为群$\langle G;*\rangle$的**阶**。若G是无限集，则称$\langle G;*\rangle$为**无限群**。

定义5-11 对于群$\langle G;*\rangle$的元素a，若存在一正整数r，使得$a^r=e$，则称元素a具有有限周期，而使$a^r=e$成立的最小的正整数称为a的**周期**。如果对于任何正整数r，总有$a^r\neq e$，则称a的周期为无限。

显然，单位元的周期是1。

定理5-5 设$\langle G;*\rangle$是一由元素g生成的循环群，

(1) 若g的周期为n，则$\langle G;*\rangle$是一个n阶的有限循环群；

(2) 若g的周期为无限，则$\langle G;*\rangle$是一个无限阶的循环群。

证明 (1) 设g的周期为n，则$g^n=e$。对于任一元素$g^K\in G$，令$K=nq+r\quad(0\leqslant r<n)$，则

$$g^K=g^{nq+r}=(g^n)^q*g^r=e*g^r=g^r,$$

即$\langle G;*\rangle$中任一元素都可写成g^r，而$0\leqslant r<n$，这说明G中至多只有n个不同的元素$g,g^2,\cdots,g^n(=e)$。

今假设n个元素$g,g^2,\cdots,g^n$中有某两个元素相同，$g^i=g^j(1\leqslant i<j\leqslant n)$，则$g^{j-i}=e$。由于$0<j-i<n$，这与$g$的周期为$n$矛盾。因此$g,g^2,\cdots,g^n$是$G$中$n$个互不相同的元素。

由上所证可知，$\langle G;*\rangle$是一个n阶的有限循环群。

(2) 设g的周期为无限，并假设$\langle G;*\rangle$是一个n阶的有限循环群(n为正整数)，则在$g,g^2,\cdots,g^n,g^{n+1}$中至少有两个元素是相同的，设为$g^i=g^j(1\leqslant i<j\leqslant n+1)$，则$g^{j-i}=e$，而$0<j-i$。这

说明 g 具有有限周期，与假设矛盾．因此，$\langle G;*\rangle$ 是一个无限阶的循环群．证完．

因为群中每一个元素都是可逆的，所以在阶大于 1 的群中没有零元．另外，除了单位元以外，群没有任何幂等元．为了说明这点，我们假定 $a\in G$ 是幂等元，于是有 $a*a=a$，则

$$a=(a^{-1}*a)*a=a^{-1}*(a*a)=a^{-1}*a=e.$$

§5.3 群的基本性质

在这节里，我们讨论群的一些重要性质．

定理 5-6 如果 $\langle G;*\rangle$ 是一个群，则对于任意的 $a,b\in G$，

(a) 存在唯一的元素 $x\in G$，使得 $a*x=b$；

(b) 存在唯一的元素 $y\in G$，使得 $y*a=b$．

证明 (a) 因为 $a*(a^{-1}*b)=(a*a^{-1})*b=e*b=b$．所以至少存在一个元素 $x=a^{-1}*b$，满足 $a*x=b$．现设 $x'\in G$ 也使得 $a*x'=b$ 成立，则

$$x'=e*x'=(a^{-1}*a)*x'=a^{-1}*(a*x')=a^{-1}*b.$$

因此，$x=a^{-1}*b$ 是满足 $a*x=b$ 的唯一元素．

(b) 用类似的方法可以证明 $y=b*a^{-1}$ 是 G 中满足 $y*a=b$ 的唯一元素．证完．

定理 5-7 如果 $\langle G;*\rangle$ 是一个群，则对于任意的 $a,b,c\in G$，

(a) 若 $a*b=a*c$，则有 $b=c$；

(b) 若 $b*a=c*a$，则有 $b=c$．

该定理是定理 5-6 的一个直接推论．它说明群满足消去律．由上述定理可知，在群 $\langle G;*\rangle$ 的运算表中，任一给出的行和任一给出的列内，G 的每一元素都必然出现一次且只能出现一次．因此群 $\langle G;*\rangle$ 的运算表的每一行和每一列都是 G 的元素的一个排列或置换．

定理 5-8　如果 $\langle G;*\rangle$ 是一个群，则对于任意的 $a,b\in G$,

$$(a*b)^{-1}=b^{-1}*a^{-1}.$$

证明　因为 $(a*b)*(a*b)^{-1}=e$, 而

$$(a*b)*(b^{-1}*a^{-1})=a*(b*b^{-1})*a^{-1}=a*a^{-1}=e.$$

故由定理5-7，有$(a*b)^{-1}=b^{-1}*a^{-1}$. 证完

用归纳法很容易将定理 5-8 的结论推广到任意 n 个元素的情形．即对于任意 $a_1,a_2,\cdots,a_n\in G$,
有

$$(a_1*a_2*\cdots*a_n)^{-1}=a_n^{-1}*a_{n-1}^{-1}*\cdots*a_2^{-1}*a_1^{-1}.$$

特别，当$\langle G;*\rangle$是阿贝尔群时，上式又可写成

$$(a_1*a_2*\cdots*a_n)^{-1}=a_1^{-1}*a_2^{-1}*\cdots*a_n^{-1}.$$

定理 5-9　若群 $\langle G;*\rangle$ 的元素 a 具有有限周期 r，则当且仅当 k 是 r 的倍数时，$a^k=e$.

证明　设 $k=mr$（m 为一整数），则

$$a^k=a^{mr}=(a^r)^m=e^m=e.$$

反之，假定 $a^k=e$，并设 $k=mr+i\ (0\leqslant i<r)$，则有 $a^i=a^{k-mr}=a^k*a^{-mr}=e*e^{-m}=e*e=e$，因为 $0\leqslant i<r$，而由假设，r 是使 $a^r=e$ 的最小正整数，所以必有 $i=0$，因此 $k=mr$．证完．

于是，若 $a^r=e$，并且对于 r 的因子 $d\ (1<d<r)$，我们有 $a^d\neq e$，则 r 是 a 的周期．例如，若 $a^8=e$，且 $a^2\neq e$，$a^4\neq e$，则 8 必定是 a 的周期．

定理 5-10　群中任一元素与它的逆元具有相同的周期．

证明　若 a 是一具有有限周期 r 的元素，则 $a^r=e$，并由此有

$$(a^{-1})^r=(a^r)^{-1}=e^{-1}=e.$$

因此，a^{-1} 必有有限周期，设为 r'，则有 $r'\leqslant r$.

又

$$a^{r'}=((a^{-1})^{r'})^{-1}=e^{-1}=e,$$

所以又有 $r\leqslant r'$．最后得 $r=r'$．证完．

由上述证明可知，当元素 a 的周期为无限时，a^{-1} 的周期也为无限。

定理 5-11 在有限群 $\langle G;*\rangle$ 中，每个元素有一有限周期．而且每个元素的周期不超过 $\# G$。

证明 设 a 是 G 中的任一元素．因为 $\langle G;*\rangle$ 是有限群，所以在序列 $a, a^2, \cdots, a^{(\# G)+1}$ 中，至少有两个元素是相同的，设 $a^p = a^r$ $(1 \leqslant p < r \leqslant (\# G)+1)$，则

$$a^{r-p} = a^r * a^{-p} = a^p * a^{-p} = a^0 = e, \quad (0 < r-p \leqslant \# G).$$

因此，a 的周期至多是 $r-p \leqslant \# G$．证完。

然而当 $\langle G;*\rangle$ 是无限群时，G 中的元素的周期不一定是有限，例如在群 $\langle I;+\rangle$ 中，除单位元 0 外，其它元素的周期都为无限。

§5.4 子群及其陪集

类似于子半群和子独异点，我们有子群的概念。

定义 5-12 设 $\langle G;*\rangle$ 是一个群，$\langle H;*\rangle$ 是 $\langle G;*\rangle$ 的子代数，如果

(1) 单位元 $e \in H$；

(2) 对于任意的 $a \in H$，有 $a^{-1} \in H$，

则称 $\langle H;*\rangle$ 是 $\langle G;*\rangle$ 的**子群**．如果 H 是 G 的真子集，则称子群 $\langle H;*\rangle$ 是 $\langle G;*\rangle$ 的**真子群**。

由定义，群 $\langle G;*\rangle$ 的任一子群本身也是一个群。

对于任意群 $\langle G;*\rangle$，$\langle G;*\rangle$ 和 $\langle \{e\};*\rangle$ 都是 $\langle G;*\rangle$ 的子群。我们称它们为群 $\langle G;*\rangle$ 的**平凡子群**。

例 1 对于群 $\langle I;+\rangle$，定义集合 $N_e = \{2, 4, 6, \cdots\}$，显然 $\langle N_e;+\rangle$ 是 $\langle I;+\rangle$ 的子代数．但单位元 $0 \notin N_e$，且对于任意的元素 $a \in N_e$，a 的逆元 $-a \notin N_e$，因此 $\langle N_e;+\rangle$ 不是 $\langle I;+\rangle$ 的子群。

$\langle Z;+\rangle$ 是 $\langle I;+\rangle$ 的子代数，且单位元 $0 \in Z$，但对于 Z 中任

一元素 $a(\neq 0)$，a 的逆元 $-a\notin Z$，因此$\langle Z;+\rangle$ 也不是 $\langle I;+\rangle$ 的子群。

定义集合$I_6=\{6i|i\in I\}$，显然 $\langle I_6;+\rangle$ 是$\langle I;+\rangle$的子代数，且 $0\in I_6$，又对于任一元素 $6i\in I_6$，有 $6(-i)=-6i\in I_6$，所以$\langle I_6;+\rangle$ 是 $\langle I;+\rangle$ 的子群。一般地，对于任意整数 m，$\langle I_m;+\rangle$ 是$\langle I;+\rangle$的子群。

事实上，定义 5-12 中关于单位元的要求是多余的。因为由 $a\in H$，根据（2）有$a^{-1}\in H$，因而有 $a*a^{-1}=e\in H$，这样我们就证明了下面的结论。

定理 5-12 设 $\langle H;*\rangle$ 是群 $\langle G;*\rangle$ 的子代数，则当且仅当对于任意的 $a\in H$，有 $a^{-1}\in H$ 时，$\langle H;*\rangle$ 是 $\langle G;*\rangle$ 的子群。

于是，若给定一群 $\langle G;*\rangle$，为了确定G的任一非空子集H是否构成 $\langle G;*\rangle$ 的一个子群，只须检验以下两条是否成立：

（1）封闭性：对于任意的 $a,b\in H$，有$a*b\in H$；

（2）可逆性：对于任意的 $a\in H$，有 $a^{-1}\in H$。

我们还可以把上述两个条件合并成为一个条件。即有

定理 5-13 设 $\langle G;*\rangle$ 是一个群，H是G的一非空子集，则当且仅当由 $a,b\in H$，可得 $a*b^{-1}\in H$时，$\langle H;*\rangle$ 是 $\langle G;*\rangle$ 的子群。

证明 设$\langle H;*\rangle$是群$\langle G;*\rangle$的子群，由定义5-12，若$a,b\in H$，则 $b^{-1}\in H$，因而$a*b^{-1}\in H$。

反之，设由元素 $a,b\in H$，可得 $a*b^{-1}\in H$ 之条件成立，则由 $a\in H$，可知 $a*a^{-1}=e\in H$，且 $e*a^{-1}=a^{-1}\in H$，这就证明了可逆性。其次，如果 $a,b\in H$，则由上所证$b^{-1}\in H$，因此 $a*(b^{-1})^{-1}=a*b\in H$，这就证明了封闭性。故由定理 5-12 可知，$\langle H;*\rangle$ 是群 $\langle G;*\rangle$ 的子群。证完。

特别，如果 $\langle G;*\rangle$ 是有限群，那么定理 5-12 中可逆性的要求也是多余的。即有

定理 5-14 设$\langle G;*\rangle$是一个有限群，若$\langle H;*\rangle$是$\langle G;*\rangle$的子

代数. 则 $\langle H;*\rangle$ 是 $\langle G;*\rangle$ 的子群.

证明 设 $a\in H$, 由定理5-11, a 有一有限周期, 设为 r。又因为 H 对运算 $*$ 是封闭的, 所以元素 $a,a^2,\cdots,a^{r-1}$, a^r 均在 H 中, 其中

$$a^{r-1}=a^r*a^{-1}=e*a^{-1}=a^{-1},$$

因此有 $a^{-1}\in H$。故 $\langle H;*\rangle$ 是 $\langle G;*\rangle$ 的子群. 证完。

于是, 若给定一有限群 $\langle G;*\rangle$, 为了确定G的某一非空子集 H 能否构成 $\langle G;*\rangle$ 的一个子群, 只需检验 H 对运算 $*$ 是否封闭即可。

定理5-14的条件还可以削弱, 即只要 H 是G的有限子集合, 而并不一定要求 $\langle G;*\rangle$ 是有限群, 子代数 $\langle H;*\rangle$ 也能成为 $\langle G;*\rangle$ 的子群。

定理5-15 设 $\langle G;*\rangle$ 是一个群。$\langle H;*\rangle$ 是 $\langle G;*\rangle$ 的有限子代数, 则 $\langle H;*\rangle$ 是 $\langle G;*\rangle$ 的子群。

对定理5-14的证明略加修改, 便可类似地给出本定理的证明.

显然, 任一阿贝尔群的子群也必为阿贝尔群。

例2 在§5.2例4中 $\{1,\alpha\}$ 对运算 $\circ$ 是封闭的(见表5-2)。因此 $\langle\{1,\alpha\};\circ\rangle$ 是 $\langle\{1,\alpha,\beta,\gamma,\delta,\varepsilon\};\circ\rangle$ 的子群. 类似地, 因为 $\{1,\gamma,\delta\}$ 对于运算 $\circ$ 也是封闭的, 所以 $\langle\{1,\gamma,\delta\};\circ\rangle$ 也是 $\langle\{1,\alpha,\beta,\gamma,\delta,\varepsilon\};\circ\rangle$ 的子群。

表5-4和表5-5分别给出了这两个子群的运算 $\circ$ 的定义(请自己识别另一些子群)。

表5-4

$\circ$	1	α
1	1	α
α	α	1

表5-5

$\circ$	1	γ	δ
1	1	γ	δ
γ	γ	δ	1
δ	δ	1	γ

事实上，对任一群 $\langle G;*\rangle$，若群 $\langle G;*\rangle$ 的子代数 $\langle H;*\rangle$ 也是一个群，则 $\langle H;*\rangle$ 一定是 $\langle G;*\rangle$ 的子群。因为，如果我们假设 e' 是群 $\langle H;*\rangle$ 的单位元，则有 $e'*e'=e'$。因而，群 $\langle G;*\rangle$ 的单位元 $e=(e')^{-1}*e'=(e')^{-1}*(e'*e')=((e')^{-1}*e')*e'=e*e'=e'$。即 $e\in H$。又若 $a\in H$，并设 a' 是 a 在 H 内的逆元，于是有 $a*a'=e$。另一方面又有 $a*a^{-1}=e$，由消去律有 $a'=a^{-1}$。即有 $a^{-1}\in H$。

这样一来，对任一群 $\langle G;*\rangle$ 来说，若 H 是 G 的一个非空子集，且 $\langle H;*\rangle$ 成群，则 $\langle H;*\rangle$ 是 $\langle G;*\rangle$ 的子群；反之，若 $\langle H;*\rangle$ 是 $\langle G;*\rangle$ 的子群，则 $\langle H;*\rangle$ 也一定是一个群。于是，$\langle H;*\rangle$ 是 $\langle G;*\rangle$ 的子群的充要条件是：$\langle H;*\rangle$ 是一个群。因此在许多数学书中常这样来定义子群：设 $\langle G;*\rangle$ 是一个群，H 是 G 的一个非空子集，若 $\langle H;*\rangle$ 也是一个群，则称 $\langle H;*\rangle$ 是群 $\langle G;*\rangle$ 的子群。

下面我们考虑群 $\langle G;*\rangle$ 中与子群 $\langle H;*\rangle$ 有关的这样一些子集。

定义 5-13 设 $\langle H;*\rangle$ 是群 $\langle G;*\rangle$ 的子群，a 是 G 的任意一个元素，则集合

$$H*a=\{h*a \mid h\in H\}$$

称为子群 $\langle H;*\rangle$ 在群 $\langle G;*\rangle$ 中的一个**右陪集**。集合

$$a*H=\{a*h \mid h\in H\}$$

称为子群 $\langle H;*\rangle$ 在群 $\langle G;*\rangle$ 中的一个**左陪集**。

如果 $a\in H$，则 $H*a=a*H=H$。这就是说，H 自身是一个右陪集且也是一个左陪集。

例 3 考虑 §5.2 例 4 中的 3 次对称群 $\langle P;\circ\rangle=\langle\{1,\alpha,\beta,\gamma,\delta,\varepsilon\};\circ\rangle$ 和它的子群 $\langle\{1,\alpha\};\circ\rangle$。在 $\langle P;\circ\rangle$ 中该子群的右陪集是：

$$\{1,\alpha\}\circ 1=\{1,\alpha\},\qquad \{1,\alpha\}\circ\gamma=\{\gamma,\beta\},$$
$$\{1,\alpha\}\circ\alpha=\{\alpha,1\},\qquad \{1,\alpha\}\circ\delta=\{\delta,\varepsilon\},$$
$$\{1,\alpha\}\circ\beta=\{\beta,\gamma\},\qquad \{1,\alpha\}\circ\varepsilon=\{\varepsilon,\delta\}.$$

于是 $\langle\{1,\alpha\};\circ\rangle$ 在 $\langle P;\circ\rangle$ 中有三个相异的右陪集：$\{1,\alpha\}$，$\{\beta,\gamma\}$，$\{\delta,\varepsilon\}$。

在 $\langle P;\circ\rangle$ 中 $\langle\{1,\alpha\};\circ\rangle$ 的左陪集是：

$1\circ\{1,\alpha\}=\{1,\alpha\}$，　　　　$\gamma\circ\{1,\alpha\}=\{\gamma,\varepsilon\}$，

$\alpha\circ\{1,\alpha\}=\{\alpha,1\}$，　　　　$\delta\circ\{1,\alpha\}=\{\delta,\beta\}$，

$\beta\circ\{1,\alpha\}=\{\beta,\delta\}$，　　　　$\varepsilon\circ\{1,\alpha\}=\{\varepsilon,\gamma\}$。

于是 $\langle\{1,\alpha\};\circ\rangle$ 在 $\langle P;\circ\rangle$ 中有三个相异的左陪集：$\{1,\alpha\}$，$\{\beta,\delta\}$，$\{\gamma,\varepsilon\}$。

考虑群 $\langle P;\circ\rangle$ 的子群 $\langle\{1,\gamma,\delta\};\circ\rangle$，在 $\langle P;\circ\rangle$ 中该子群的右陪集是：

$\{1,\gamma,\delta\}\circ 1=\{1,\gamma,\delta\}$，　　$\{1,\gamma,\delta\}\circ\gamma=\{\gamma,\delta,1\}$，

$\{1,\gamma,\delta\}\circ\alpha=\{\alpha,\varepsilon,\beta\}$，　　$\{1,\gamma,\delta\}\circ\delta=\{\delta,1,\gamma\}$，

$\{1,\gamma,\delta\}\circ\beta=\{\beta,\alpha,\varepsilon\}$，　　$\{1,\gamma,\delta\}\circ\varepsilon=\{\varepsilon,\beta,\alpha\}$。

于是 $\langle\{1,\gamma,\delta\};\circ\rangle$ 在 $\langle P;\circ\rangle$ 中有两个相异的右陪集：$\{1,\gamma,\delta\}$，$\{\alpha,\beta,\varepsilon\}$。

容易验证，对于每一个 $a\in\{1,\alpha、\beta,\gamma,\delta,\varepsilon\}$，我们有 $\{1,\gamma,\delta\}\circ a=a\circ\{1,\gamma,\delta\}$。

定义 5-14　设 $\langle H;*\rangle$ 是群 $\langle G;*\rangle$ 的子群，如果对于每一个 $a\in G$，有 $a*H=H*a$，则称 $\langle H;*\rangle$ 是群 $\langle G;*\rangle$ 的**正规子群**。此时右陪集和左陪集简称为**陪集**。

上例中，$\langle\{1,\gamma,\delta\};\circ\rangle$ 是群 $\langle P;\circ\rangle$ 的正规子群。但 $\langle\{1,\alpha\};\circ\rangle$ 不是 $\langle P;\circ\rangle$ 的正规子群。下面给出判别一个子群为正规子群的条件。为此我们先引进下面的符号。

设 H 是群 $\langle G;*\rangle$ 中 G 的一个子集。对于任一元素 $a\in G$，我们用符号 $a*H*a^{-1}$ 表示下面的集合

$$a*H*a^{-1}=\{a*h*a^{-1}\mid h\in H\}。$$

一般地，若 A、B 是 G 的子集，我们定义

$$A*B=\{a*b\mid a\in A,b\in B\}。$$

定理 5-16　设 $\langle H;*\rangle$ 是群 $\langle G;*\rangle$ 的一个子群，当且仅当对于任意的 $a\in G$，有 $a*H*a^{-1}=H$ 时，$\langle H;*\rangle$ 是 $\langle G;*\rangle$ 的正规子群。

证明 设$\langle H;*\rangle$是$\langle G;*\rangle$的正规子群，则对于任意的$a\in G$，有$a*H=H*a$。因此，由运算$*$的可结合性和符号$a*H*a^{-1}$的定义可知

$$a*H*a^{-1}=(a*H)*a^{-1}=(H*a)*a^{-1}=H*(a*a^{-1})=H*e=H.$$

反之，假设对任意的$a\in G$，有$a*H*a^{-1}=H$，则$H*a=(a*H*a^{-1})*a=(a*H)*(a^{-1}*a)=(a*H)*e=a*H$，即$\langle H;*\rangle$是$\langle G;*\rangle$的正规子群。证完。

上述$\langle H;*\rangle$为正规子群的充要条件还可以削弱，即有

定理 5-17 设$\langle H;*\rangle$是群$\langle G;*\rangle$的一个子群，当且仅当对于任意的$a\in G$，有$a*H*a^{-1}\subseteq H$时，$\langle H;*\rangle$是$\langle G;*\rangle$的正规子群。

证明 必要性显然成立。

设对任意的$a\in G$，$a*H*a^{-1}\subseteq H$， (1)

由于$a^{-1}\in G$，因此以a^{-1}代a仍有$a^{-1}*H*a\subseteq H$成立。以a左乘，以a^{-1}右乘得

$$a*(a^{-1}*H*a)*a^{-1}\subseteq a*H*a^{-1},$$

即

$$H\subseteq a*H*a^{-1}. \quad (2)$$

由(1)和(2)得 $a*H*a^{-1}=H$。

因而由定理5-16，$\langle H;*\rangle$是正规子群。证完。

在上例中我们发现，子群$\langle\{1,\alpha\};\circ\rangle$在$\langle P;\circ\rangle$中所有相异的右陪集和所有相异的左陪集分别组成$P$的一个分划。子群$\langle\{1,\gamma,\delta\};\circ\rangle$在$\langle P;\circ\rangle$中的所有相异的陪集也组成$P$的一个分划。这一结论是否具有一般性呢？即群的子群在该群中的所有相异右(左)陪集是否一定组成该群之域的分划呢？回答是肯定的。为此，我们先证明下面的定理。

定理 5-18 设$\langle H;*\rangle$是群$\langle G;*\rangle$的子群，则

(1) 当且仅当$b*a^{-1}\in H$时，$b\in H*a$；

(2) 当且仅当$a^{-1}*b\in H$时，$b\in a*H$。

证明 (1) 当且仅当存在某一$h\in H$，使得$b=h*a$时，有

$b \in H*a$。由此，当且仅当存在某一 $h \in H$，使得 $b*a^{-1}=h$ 时，有 $b \in H*a$。这即是当且仅当 $b*a^{-1} \in H$ 时，有 $b \in H*a$。

（2）的证明与（1）的证明类似。证完。

定理5-19 设 $\langle H;*\rangle$ 是群 $\langle G;*\rangle$ 的一个子群，a 和 b 是G的任意两个元素，则有

（1）$H*a=H*b$ 或者 $(H*a)\cap(H*b)=\phi$；

（2）$a*H=b*H$ 或者 $(a*H)\cap(b*H)=\phi$。

证明 （1）设 $(H*a)\cap(H*b)\neq\phi$，并设 $x\in(H*a)\cap(H*b)$，则 $x=h_1*a=h_2*b$ $(h_1,h_2\in H)$。而 $e=x^{-1}*x=a^{-1}*h_1^{-1}*h_2*b$，因此，$a*b^{-1}=h_1^{-1}*h_2\in H$，由定理 5-18，$a\in H*b$，因此 $a=h*b$ $(h\in H)$。对 $H*a$ 中任一元素 h_3*a，有 $h_3*a=h_3*(h*b)=(h_3*h)*b\in H*b$，因此 $H*a\subseteq H*b$。类似地有 $e=x^{-1}*x=b^{-1}*h_2^{-1}*h_1*a$，$b*a^{-1}=h_2^{-1}*h_1\in H$，于是 $b\in H*a$，因此又有 $H*b\subseteq H*a$。故 $H*a=H*b$。

（2）的证明与（1）的证明类似。证完。

对于群 $\langle G;*\rangle$ 中的任意两个元素 a 和 b，在什么情形下有 $H*a=H*b$，在什么情形下有 $(H*a)\cap(H*b)=\phi$ 呢？关于这，我们有下面的定理。

定理 5-20 设 $\langle H;*\rangle$ 是群 $\langle G;*\rangle$ 的一个子群，则

（1）当且仅当 $b\in H*a$ 时，$H*b=H*a$；

（2）当且仅当 $b\in a*H$ 时，有 $b*H=a*H$。

证明 （1）设 $b\in H*a$，又因为 $e\in H$，所以 $b=e*b\in H*b$。于是 $(H*a)\cap(H*b)\neq\phi$，由定理 5-19，$H*b=H*a$。

反之，设 $H*b=H*a$，则由 $b=e*b\in H*b$ 可知 $b\in H*a$。

（2）的证明与（1）的证明类似。证完。

定理 5-20 说明，由元素 a 所确定的 $\langle H;*\rangle$ 的右（左）陪集与该右（左）陪集中任一元素 b 所确定的右（左）陪集相同。由元素 a 所确定的 $\langle H;*\rangle$ 的右（左）陪集与该右（左）陪集以外的任一元

素 b 所确定的右（左）陪集相交为空。

定理5-21 设 $\langle H;*\rangle$ 是群 $\langle G;*\rangle$ 的子群，则

(1) $\langle G;*\rangle$ 中 $\langle H;*\rangle$ 的所有相异的右陪集组成 G 的一个分划；

(2) $\langle G;*\rangle$ 中 $\langle H;*\rangle$ 的所有相异的左陪集组成 G 的一个分划.

证明 (1) 因为 $\langle H;*\rangle$ 是群 $\langle G;*\rangle$ 的子群，有 $e\in H$，所以对任一 $a\in G$，有 $a=e*a\in H*a$，即 $H*a$ 非空，又由定理 5-19(1)，$\langle G;*\rangle$ 中 $\langle H;*\rangle$ 的任意两个相异的右陪集相交为 ϕ，而且每一元素 $a\in G$ 必在右陪集 $H*a$ 中，因此 H 的所有相异的右陪集组成 G 的一个分划。

(2) 的证明与 (1) 的证明类似. 证完。

定理 5-21 中的分划称为群 $\langle G;*\rangle$ 中与 $\langle H;*\rangle$ 相关的**右（左）陪集分划**。这种分划可看作是由 G 上某一等价关系 ρ 所导致的等价分划，这里 ρ 是当且仅当 a 和 b 是在 $\langle H;*\rangle$ 的相同的右（左）陪集中时，有 $a\rho b$。当 $\langle H;*\rangle$ 是 $\langle G;*\rangle$ 的正规子群时，这种分划简单地称为 $\langle G;*\rangle$ 中与 $\langle H;*\rangle$ 相关的**陪集分划**。

上述这些定理还给出了构造右（左）陪集分划的方法。若 $\langle H;*\rangle$ 是 $\langle G;*\rangle$ 的真子群，则必有一元素 $a_1\in G$ 而 $a_1\notin H$，于是作 H 的右陪集 $H*a_1$（或左陪集 a_1*H），如果 G 的子集 $H\cup H*a_1$（或 $H\cup a_1*H$）还不能包含 G 的全部元素，则再取一不属于 $H\cup H*a_1$（或 $H\cup a_1*H$）的 G 之一元 a_2，并作右陪集 $H*a_2$（或 a_2*H），若 G 中还有元素不属于子集合 $H\cup H*a_1\cup H*a_2$（或 $H\cup a_1*H\cup a_2*H$），设 a_3 是这样的一个元素，则与上面同样，可作右陪集 $H*a_3$（或 a_3*H），继续这样作下去，有可能把集合 G 分划成有限多个右(左)陪集的并，如

$$G=H*a_0\cup H*a_1\cup\cdots\cup H*a_n,$$

或 $$G=a_0*H\cup a_1*H\cup\cdots\cup a_n*H,\qquad (a_0\in H\text{、所以 }H*a_0=H)。$$

但 G 亦有可能不能分划成有限多个右（左）陪集的并。例如，当

$\langle H;*\rangle=\langle\{e\};*\rangle$ 而 $\langle G;*\rangle$ 是无限群时，就会发生这种现象。

对于任一 $a\in G$，定义一从 H 到 $H*a$ 的函数 f：$H\to H*a$。使得对于每一个 $h\in H$，有 $f(h)=h*a$。由定理 5-7 可知，这是一个由 H 到 $H*a$ 的双射，因此，$H*a$ 与 H 具有相同的基数。同样 $a*H$ 与 H 也具有相同的基数。不仅如此，我们还有下面的结论，即 $\langle H;*\rangle$ 的所有相异右陪集的个数和所有相异左陪集的个数是相同的。

事实上，若 $\langle H;*\rangle$ 的所有相异右陪集的个数为有限数 n 个，设为 $H*a_1$，$H*a_2,\cdots,H*a_n$，则 $a_1^{-1}*H$，$a_2^{-1}*H,\cdots,a_n^{-1}*H$ 必为 $\langle H;*\rangle$ 的所有相异的左陪集，为此要证明以下两点：①任意两个左陪集 $a_i^{-1}*H\neq a_j^{-1}*H\ (i\neq j)$；②$G$ 中任一元素 g 必在某个左陪集 $a_i^{-1}*H$ 中 $(1\leqslant i\leqslant n)$。

假设在 $i\neq j$ 时 $(1\leqslant i,\ j\leqslant n)$，有 $a_i^{-1}*H=a_j^{-1}*H$，则由定理 5-20，有 $a_i^{-1}\in a_j^{-1}*H$，又由定理 5-18，有 $a_j*a_i^{-1}\in H$，从而有 $a_j\in H*a_i$，于是由定理 5-20，有 $H*a_i=H*a_j$。这与假设矛盾，所以 $a_i^{-1}*H\neq a_j^{-1}*H\ (i\neq j)$。

对任一元素 $g\in G$，有 $g^{-1}\in G$，因此 g^{-1} 必在某个右陪集 $H*a_i$ 中，即 $g^{-1}=h*a_i\ (h\in H)$，于是 $g=(h*a_i)^{-1}=a_i^{-1}*h^{-1}\in a_i^{-1}*H$ $(1\leqslant i\leqslant n)$。

用同样的方式亦可证明：当 $\langle H;*\rangle$ 的所有相异的左陪集为 n 个时，$\langle H;*\rangle$ 的所有相异右陪集也是 n 个。因此当一方为无限时，另一方也为无限。

定义 5-15 设 $\langle H;*\rangle$ 是群 $\langle G;*\rangle$ 的子群，群 $\langle G;*\rangle$ 中 $\langle H;*\rangle$ 的所有相异右（左）陪集的个数称为 $\langle H;*\rangle$ 在 $\langle G;*\rangle$ 中的**指数**。

例 3 中，$\langle\{1,\alpha\};\circ\rangle$ 在 $\langle P;\circ\rangle$ 中的指数是 3，$\langle\{1,\gamma,\delta\};\circ\rangle$ 在 $\langle P;\circ\rangle$ 中的指数是 2 。

由上面的讨论，我们可以得到如下的定理。

定理 5-22 （拉格朗日定理）

设 $\langle G;*\rangle$ 是一具有子群 $\langle H;*\rangle$ 的有限群，且 $\langle H;*\rangle$ 在 $\langle G;*\rangle$ 中的指数为 d，则 $\#G=d\cdot(\#H)$。

此定理的结论是显然的。而且由此可知有限群 $\langle G;*\rangle$ 的任一子群的阶必为该群的阶的因子。因此任何素数阶的群只有平凡子群。在此我们还可得到比定理 5-11 更进一步的结果。

定理 5-23 在有限群 $\langle G;*\rangle$ 中，每个元素的周期是 $\#G$ 的因子。

证明 设 $a\in G$，且 a 的周期为 r，则 $\langle\{e,a,a^2,\cdots,a^{r-1}\};*\rangle$ 是 $\langle G;*\rangle$ 的一个子群。由定理 5-22，r 是 $\#G$ 的因子。证完。

由上可知，若 $\langle G;*\rangle$ 是一 n 阶的有限群，那么对任何的 $a\in G$，有 $a^n=e$，若 $\langle G;*\rangle$ 是一素数阶的群，则 G 中任何非单位元素的周期恰好是 $\#G$。

§5.5 正规子群与满同态

应用代数系统的同态概念于群，可得到群之间的同态关系。

设 $\langle G;*\rangle$ 和 $\langle G';\circ\rangle$ 是两个群，f 是由 G 到 G' 的一个函数。我们知道，若对于所有的 $a,b\in G$，有

$$f(a*b)=f(a)\circ f(b),$$

则 f 是由群 $\langle G;*\rangle$ 到群 $\langle G';\circ\rangle$ 的同态。

根据 f 是内射，满射或双射，上述群之间的同态也可区分为单一同态、满同态或同构。

定理 5-24 设 $\langle G;*\rangle$ 是一个群，$\langle G';\circ\rangle$ 是一个二元代数，若 f 是由 $\langle G;*\rangle$ 到 $\langle G';\circ\rangle$ 的满同态，则 $\langle G';\circ\rangle$ 也是一个群。

这个定理用不着证明，因为根据定理 4-5，该定理的结论是显然的。

定义 5-16 设 f 是由群 $\langle G;*\rangle$ 到群 $\langle G';\circ\rangle$ 的满同态，则称

$\langle G';\circ\rangle$ 的单位元 e' 在 G 中所有象源的集合

$$K=\{a\mid a\in G,\ f(a)=e'\}$$

为满同态 f 的**核**。

定理 5-25 设 K 是由群 $\langle G;*\rangle$ 到群 $\langle G';\circ\rangle$ 的满同态 f 的核，则 $\langle K;*\rangle$ 是群 $\langle G;*\rangle$ 的正规子群。

证明 首先证明 $\langle K;*\rangle$ 是 $\langle G;*\rangle$ 的子群。显然 $\langle G;*\rangle$ 的单位元 $e\in K$，因此 K 非空。若 $a,b\in K$，则 $f(a)=f(b)=e'$，因此

$$f(a*b^{-1})=f(a)\circ f(b^{-1})=f(a)\circ[f(b)]^{-1}=e'\circ[e']^{-1}=e',$$

于是 $a*b^{-1}\in K$，因此 $\langle K;*\rangle$ 是 $\langle G;*\rangle$ 的子群。

其次，对任意的 $a\in G$ 和任意的 $k\in K$，

$$\begin{aligned}f(a*k*a^{-1})&=f(a*k)\circ f(a^{-1})=f(a)\circ f(k)\circ[f(a)]^{-1}\\&=f(a)\circ e'\circ[f(a)]^{-1}=f(a)\circ[f(a)]^{-1}=e',\end{aligned}$$

所以，对任意的 $a\in G$，$a*K*a^{-1}\subseteq K$。

于是，$\langle K;*\rangle$ 是 $\langle G;*\rangle$ 的正规子群。故定理成立。

定理 5-26 设 f 是由群 $\langle G;*\rangle$ 到群 $\langle G';\circ\rangle$ 的满同态，f 的核为 K，若 G 中元素 a 在 G' 中的象是 a'，则 a' 在 G 中所有象源的集合是陪集 $a*K$。

证明 对任一元素 $a*k\in a*K$ $(k\in K)$，

$$f(a*k)=f(a)\circ f(k)=a'\circ e'=a',$$

所以陪集 $a*K$ 中所有元素都是 a' 的象源。

再假设 b 是 a' 的象源，我们从

$$f(a^{-1}*b)=f(a^{-1})\circ f(b)=[f(a)]^{-1}\circ f(b)=(a')^{-1}\circ a'=e',$$

就得到 $a^{-1}*b\in K$。由定理 5-18，$b\in a*K$，即 b 在陪集 $a*K$ 中。因此 a' 的所有象源的集合是 $a*K$。定理得证。

于是，由群 $\langle G;*\rangle$ 到群 $\langle G';\circ\rangle$ 的一个满同态 f，就得到一个正规子群 $\langle K;*\rangle$。该正规子群的所有陪集构成 G 的一个分划，而这个分划可看作是由 G 上的某个等价关系 ρ 所导致的。这个关系 ρ 是：当且仅当 a 和 b 是在 $\langle K;*\rangle$ 的同一陪集中时，有 $a\rho b$。由于

当且仅当元素在同一陪集中时，在 f 作用下的函数值相等，因此该等价关系 ρ 就是 ρ_f。

反之，假设 $\langle K;*\rangle$ 是群 $V=\langle G;*\rangle$ 的任意一个正规子群，则导致 $\langle G;*\rangle$ 中与 $\langle K;*\rangle$ 相关的陪集分划的等价关系 ρ 是 $\langle G;*\rangle$ 上的一个同余关系（见习题第31题）。因而由定理4-9，存在一个由 V 到 V/ρ 的满同态，这里 $V/\rho=\langle G/\rho;\tilde{*}\rangle$。其中

$$G/\rho=\{a*K\mid a\in G\},$$

$$(a*K)\tilde{*}(b*K)=(a*b)*K. \qquad (5\text{-}1)$$

由定理 5-24，V/ρ 也是一个群。于是，我们给出下面的定义。

定义 5-17 群 $V=\langle G;*\rangle$ 的正规子群 $\langle K;*\rangle$ 的所有陪集对于 (5-1) 式所规定的运算构成的群，称为群 $\langle G;*\rangle$ 关于 $\langle K;*\rangle$ 的**商群**，常用记号 V/K 表示（而不用 V/ρ）。

定理 5-27 设 $\langle K;*\rangle$ 是群 $V=\langle G;*\rangle$ 的一个正规子群，则存在一个由群 V 到 V 关于 $\langle K;*\rangle$ 的商群 V/K 的满同态，这个满同态的核就是 K。

根据定理 4-9(3)，我们又直接可得下述结论。

定理 5-28 设 f 是由群 $V=\langle G;*\rangle$ 到群 $V'=\langle G';\circ\rangle$ 的一个满同态，其核是 K，则群 $V'=\langle G';\circ\rangle$ 与群 V 关于 $\langle K;*\rangle$ 的商群 V/K 同构。

习　题

1. 给出一个半群，使其具有左单位元和右零元，但又不是独异点。

2. 独异点$\langle 2^U; \cup \rangle$、$\langle 2^U; \cap \rangle$、$\langle Z; + \rangle$、$\langle Z; \cdot \rangle$、$\langle R_A; \circ \rangle$和$\langle V^*; \circ \rangle$具有零元吗？如果有，它们是什么？

3. 设有二元代数$V = \langle \{a, b, c, d\}; \cdot \rangle$，其中运算$\cdot$由下表定义。

$\cdot$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

(1) 证明V是一循环独异点，并列出它的生成元；

(2) 如果g是生成元，将V的每一元素表示成g的幂；

(3) 列出V的所有幂等元；

(4) 证明V中每一个元素的某次乘方是幂等的。

4. 证明自然数集N对于运算$x*y = \max\{x, y\}$构成一个半群。它是独异点吗？

5. 设$S = \{a, b\}$，试证半群$\langle S^S; \circ \rangle$是不可交换的，这里$\circ$是函数的复合运算。

6. 试证，每一个有限半群都有一个幂等元。

7. 证明在一个独异点中左可逆元（右可逆元）的集合形成一个子独异点。

8. 设$\langle S; * \rangle$是一个半群，如果对于所有的$x, y \in S$，由$a*x = a*y \Rightarrow x = y$，则元素$a \in S$称为左可约的。证明：若$a$和$b$是左可约的，则$a*b$也是左可约的。

9. 试证明一独异点的所有可逆元素的集合，对于该独异点所具有的运算，能够构成群。

10. 下列的二元代数 $\langle G;*\rangle$ 中哪一个构成群？在 $\langle G;*\rangle$ 是群的情况下，指出其单位元并确定每个元素的逆。

(1) $G=\{1,10\}$，$*$ 是按模 11 的乘法；

(2) $G=\{1,3,4,5,9\}$，$*$ 是按模 11 的乘法；

(3) $G=Q$，$*$ 是通常的加法；

(4) $G=Q$，$*$ 是通常的乘法；

(5) $G=I$，$*$ 是通常的减法；

(6) $G=\{\alpha,\beta,\gamma,\delta\}$，$*$ 是下面定义的运算

*	α	β	γ	δ
α	β	δ	α	γ
β	δ	γ	β	α
γ	α	β	γ	δ
δ	γ	α	δ	β

11. 如果 $\langle G;*\rangle$ 是一个阿贝尔群，则对于所有的 $a,b\in G$，证明 $(a*b)^n=a^n*b^n\ (n\in N)$。

12. 试证明在一个群 $\langle G;*\rangle$ 中，如果对于任意的 $a,b\in G$，有 $(a*b)^2=a^2*b^2$，则 $\langle G;*\rangle$ 必定是一个阿贝尔群。

13. 试证明如果一个群的每一个元素都是它自己的逆元，则该群必是阿贝尔群。

14. 试证明 $\langle\{1\};\cdot\rangle$ 和 $\langle\{1,-1\};\cdot\rangle$ 是非零实数在乘法运算下仅有的有限群。

15. 试证明 x 的所有多项式的集合在加法运算下是一个群。

16. 试证明 $\langle Z_3;\oplus_3\rangle$ 是一个群，其中 $Z_3=\{0,1,2\}$，$\oplus_3$ 是按模 3 的加法。

17. 试证明在一个有限群里，周期大于 2 的元素的个数一定是

偶数。

18。设 $\langle G;*\rangle$ 是一个阶为偶数的有限群，试证明在 G 里周期等于 2 的元素的个数一定是奇数。

19。设 $\langle G;*\rangle$ 是循环群，f 是从 $\langle G;*\rangle$ 到 $\langle G';\circ\rangle$ 的满同态（$\circ$ 是二元运算），试证明 $\langle G';\circ\rangle$ 也是循环群。

20。设 $\langle G;*\rangle$ 是无限阶的循环群，$\langle G';\circ\rangle$ 是任意循环群，试证明存在由 $\langle G;*\rangle$ 到 $\langle G';\circ\rangle$ 的同态。

21。设 $\langle G;*\rangle$ 是一个由 g 生成的阶为 n 的有限循环群，证明 g^r 也生成 $\langle G;*\rangle$（这里 r 与 n 互素）。

22。试证明所有无限阶的循环群都相互同构。又凡阶等于 n 的有限循环群也都相互同构。

23。设 $\langle H_1;*\rangle$ 和 $\langle H_2;*\rangle$ 是群 $\langle G;*\rangle$ 的子群，G 的子集 H_1*H_2 是否能构成 $\langle G;*\rangle$ 的子群？

24。试证明群 $\langle G;*\rangle$ 的两个子群的交集也构成 $\langle G;*\rangle$ 的子群。

25。试证明循环群的子群也是循环群。

26。试证明阶为素数的群一定是循环群。

27。试证明两个正规子群的交集还是构成正规子群。

28。设 $\langle S;*\rangle$ 是一有限可交换的独异点，并且对于任意的 $a, b, c\in S$，由 $a*b=a*c$ 可得 $b=c$，证明 $\langle S;*\rangle$ 是一交换群。

29。设 $\langle G;*\rangle$ 是一个群，$\langle \tilde{G};*\rangle$ 是 $\langle G;*\rangle$ 的一个子群，定义 G 的子集 H 为

$$H=\{a\mid a*\tilde{G}=\tilde{G}*a\},$$

证明：(1) $\langle H;*\rangle$ 是 $\langle G;*\rangle$ 的子群。

(2) $\langle \tilde{G};*\rangle$ 是 $\langle H;*\rangle$ 的正规子群。

30。设 $\langle G;*\rangle$ 是一个群，定义 G 的子集 H 为

$$H=\{a\mid a*x=x*a, \text{对于任意的 } x\in G\},$$

证明 $\langle H;*\rangle$ 是 $\langle G;*\rangle$ 的子群。

31。设 $\langle G;*\rangle$ 是一个群，$\langle H;*\rangle$ 是 $\langle G;*\rangle$ 的一个正规子群，证

明导致$\langle G;*\rangle$中与$\langle H;*\rangle$相关的陪集分划的等价关系ρ是$\langle G;*\rangle$上的一个同余关系。

32．设g是由群$\langle G;*\rangle$到群$\langle G';\circ\rangle$的满同态。试证明：

(1) 若$\langle H;*\rangle$是群$\langle G;*\rangle$的子群，则H的象H'对于运算$\circ$也构成$\langle G';\circ\rangle$的子群。

(2) 若$\langle N;*\rangle$是群$\langle G;*\rangle$的正规子群，则N的象N'对于运算$\circ$也构成$\langle G';\circ\rangle$的正规子群。

33．设g是由群$\langle G;*\rangle$到群$\langle G';\circ\rangle$的满同态，试证明：

(1) 若$\langle H';\circ\rangle$是群$\langle G';\circ\rangle$的子群，则H'的象源H对于运算$*$也构成$\langle G;*\rangle$的子群；

(2) 若$\langle N';\circ\rangle$是群$\langle G';\circ\rangle$的正规子群，则N'的象源N对于运算$*$也构成$\langle G;*\rangle$的正规子群。

34．设$V=\langle G;*\rangle$是一个循环群，$\langle N;*\rangle$是$\langle G;*\rangle$的子群，证明V/N也是循环群。

第六章 环和域

在这一章里我们继续讨论代数系统，研究具有两个二元运算的代数系统——环和域。在高等代数里我们已经看到，对于通常的加法和乘法运算，全体整数构成一个环，全体有理数，全体实数或全体复数都构成一个域。由此可见，环和域这两个概念的重要性。和对于群的讨论一样，我们这里只是对环和域作某些最基本的介绍。

环和域的知识在研究错误检测、代码校正及其物理实现上是必不可少的。

§6.1 环

定义 6-1 代数系统 $\langle R; +, \cdot \rangle$[注] 如果对于二元运算 $+$ 和 $\cdot$ 满足以下三个条件，则称为是一个**环**：

(1) $\langle R; + \rangle$ 是阿贝尔群。

(2) $\langle R; \cdot \rangle$ 是半群。

(3) 运算 $\cdot$ 对于 $+$ 是可分配的，即对于任意的 $a, b, c \in R$，

$$a \cdot (b+c) = a \cdot b + a \cdot c, \quad (b+c) \cdot a = b \cdot a + c \cdot a.$$

用归纳法很容易证明，在环 $\langle R; +, \cdot \rangle$ 中，对于任意的 $a, b_1, b_2, \cdots, b_n \in R$，

$$a \cdot (b_1 + b_2 + \cdots + b_n) = a \cdot b_1 + a \cdot b_2 + \cdots + a \cdot b_n,$$

$$(b_1 + b_2 + \cdots + b_n) \cdot a = b_1 \cdot a + b_2 \cdot a + \cdots + b_n \cdot a.$$

习惯上把环 $\langle R; +, \cdot \rangle$ 中的运算 $+$ 叫做加法，把运算 $\cdot$ 叫

[注] 在这里，R 表示一个非空集合，不表示实数集。

做乘法，虽然这些运算不一定就是通常的加法和乘法。在群中，如果一个群的运算叫做加法，并用符号+表示，那么我们就把这个群称为**加法群**，而且我们总假定一个加法群是一个交换群。环$\langle R;+,\cdot\rangle$中，R对于加法构成加法群。

在环$\langle R;+,\cdot\rangle$中，加法运算的单位元用0表示，称为**零元**。如果乘法运算有单位元，则用1表示，并称它为**单位元**。环中元素a对加法的逆元用$-a$表示，称它为a的**负元**。$a+(-b)$通常写成$a-b$。而乘法逆元如果存在的话，用a^{-1}表示，称它为a的**逆元**。积$a\cdot b$通常写成ab。对于运算+，a的n次幂表示成na，即$na=\underbrace{a+a+\cdots+a}_{n个}$。而对于运算$\cdot$，$a$的$n$次幂表示成$a^n$，即$a^n=\underbrace{a\cdot a\cdots a}_{n个}$。在没有括号时，我们约定指数优先于乘法，而乘法优先于加法。

由环的定义可以看出，一个环$\langle R;+,\cdot\rangle$中的运算$\cdot$可以满足也可以不满足以下条件：

(1) **交换律**：对于任意的$a,b\in R$，$ab=ba$。

(2) **单位元**：存在一个元素$1\in R$，使得对于所有的$a\in R$，

$$1\cdot a=a\cdot 1=a。$$

(3) **消去律**：若$a\neq 0$，则对于任意的$b,c\in R$，

由 $ab=ac$， 可推得 $b=c$，

由 $ba=ca$， 可推得 $b=c$。

定义6-2 如果环$\langle R;+,\cdot\rangle$对于运算$\cdot$满足交换律，则称环$\langle R;+,\cdot\rangle$是**交换环**。

例1 代数系统$\langle I;+,\cdot\rangle$是一个环，其中+和$\cdot$都是通常的加法和乘法。它是具有单位元1且满足消去律的交换环。

例2 $\langle I_2;+,\cdot\rangle$也是一个环，这里$I_2=\{2i\mid i\in I\}$，+和$\cdot$的意义同上。这个环不具有单位元，是一个满足消去律的交换环。

例3 $\langle Z_3;\oplus_3,\odot_3\rangle$ 是一个环，其中 $\oplus_3$ 与 $\odot_3$ 是按模3的加与乘，即

$$a\oplus_3 b=\mathrm{res}_3(a+b),\quad a\odot_3 b=\mathrm{res}_3(ab).$$

其运算表如下：

$\oplus_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\odot_3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

该环的单位元是1，而且从 $\odot_3$ 的运算表中可看出，对于任意的 $a\neq 0$，当 $b\neq c$ 时，有 $a\odot_3 b\neq a\odot_3 c$，且 $b\odot_3 a\neq c\odot_3 a$。因此该环满足消去律且是一个交换环。

类似地，$\langle Z_4;\oplus_4,\odot_4\rangle$ 也是一个环，这里 $\oplus_4$ 和 $\odot_4$ 是按模4的加与乘。其运算表如下：

$\oplus_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\odot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

它是具有单位元1的交换环。但它不满足消去律，例如 $2\odot_4 1=2\odot_4 3$。

一般来说，对于任意的正整数 m，$\langle Z_m;\oplus_m,\odot_m\rangle$ 是一个具有单位元的交换环。数0是零元，对任一 $a(\neq 0)\in Z_m$，$b=m-a$ 是其负元，0的负元是0自身。

比较环和整环的定义（参见§4.2)，我们发现，整环是一个具有单位元，满足消去律的交换环。

定理 6-1 设 $\langle R;+,\cdot\rangle$ 是一个环，则对于任意的 $a,b\in R$，

(1) $a\cdot 0=0\cdot a=0$。

(2) $(-a)\cdot b=a\cdot(-b)=-(ab)$。

证明 (1) 因为 $0\cdot a+0\cdot a=(0+0)\cdot a=0\cdot a$，

所以 $0\cdot a+0\cdot a-(0\cdot a)=0\cdot a-(0\cdot a)$。

即得 $0\cdot a=0$。

同样地有 $a\cdot 0=0$，

因此 $a\cdot 0=0\cdot a=0$。

(2)
$$
\begin{aligned}
(-a)\cdot b &= ab+(-a)\cdot b-(ab)\\
&=(a+(-a))b-(ab)\\
&=0\cdot b-(ab)\\
&=-(ab).
\end{aligned}
$$

同样地有 $a\cdot(-b)=-(ab)$。

所以 $(-a)\cdot b=a\cdot(-b)=-(ab)$。证完

(1) 说明环中加法的单位元对于乘法来说是零元。也就是说两个元素相乘，当至少有一个因子是零时，乘积一定等于零。我们将看到，这个结论的逆不成立。即可能有 $a\cdot b=0$，但 $a\neq 0$，$b\neq 0$。例如在上述例 3 环 $\langle Z_4;\oplus_4,\odot_4\rangle$ 中 $2\odot_4 2=0$。

定义 6-3 若在环 $\langle R;+,\cdot\rangle$ 里，$a\neq 0$ $b\neq 0$，但有 $ab=0$，则我们称 a 是这个环的一个**左零因子**。b 是这个环的一个**右零因子**。

上例中的 2 既是环 $\langle Z_4;\oplus_4,\odot_4\rangle$ 的一个左零因子，也是一个右零因子。显然，一个环若是交换环，则它的左零因子当然也是右零因子。但在非交换环中，一个左零因子不一定同时也是右零因子。

如果一个环没有零因子，也就是说，由 $ab=0$ 必然推出 $a=0$ 或者 $b=0$，那么这个环就称为是**无零因子环**。

定理 6-2 环 $\langle R;+,\cdot\rangle$ 成为无零因子环的充要条件是它满足消去律。

证明 设$\langle R;+,\cdot\rangle$是无零因子环，且设$a,b,c\in R$，其中$a\neq 0$使得$ab=ac$，$ba=ca$，因此$ab-(ac)=0$ $ba-(ca)=0$，从而$a(b-c)=0$ $(b-c)a=0$。因为$\langle R;+,\cdot\rangle$是无零因子环，且$a\neq 0$，所以必有$b-c=0$ 即 $b=c$。故$\langle R;+,\cdot\rangle$满足消去律。

反之，设$\langle R;+,\cdot\rangle$满足消去律，且设$a,b\in R$使$ab=0$。如果$a\neq 0$，我们有$ab=a0$，由消去律得$b=0$。因此，$\langle R;+,\cdot\rangle$是无零因子环。证完。

§6.2 子环、理想子环

类似于子群，环中也有子环的概念。

定义 6-4 如果环$\langle R;+,\cdot\rangle$的子代数$\langle \tilde{R};+,\cdot\rangle$也是一个环，则称$\langle \tilde{R};+,\cdot\rangle$是环$\langle R;+,\cdot\rangle$的**子环**。如果$\tilde{R}$是R的真子集，则称$\langle \tilde{R};+,\cdot\rangle$是$\langle R;+,\cdot\rangle$的**真子环**。

环$\langle R;+,\cdot\rangle$的子代数$\langle \tilde{R};+,\cdot\rangle$在什么条件下构成$\langle R;+,\cdot\rangle$的子环呢？由定义，$\langle \tilde{R};+\rangle$必须成群，$\langle \tilde{R};\cdot\rangle$必须成半群，且满足$\cdot$对$+$的分配律和运算$+$的可交换性。因为后三条显然是成立的，因此$\langle \tilde{R};+,\cdot\rangle$成为$\langle R;+,\cdot\rangle$的子环的充要条件是$\langle \tilde{R};+\rangle$成群，即$\langle \tilde{R};+\rangle$是$\langle R;+\rangle$的子群。因此我们有下面的定理。

定理 6-3 设$\langle R;+,\cdot\rangle$是一个环，$\langle \tilde{R};+,\cdot\rangle$是$\langle R;+,\cdot\rangle$的子代数，当且仅当$\langle \tilde{R};+,\cdot\rangle$对于运算$+$满足可逆性时，$\langle \tilde{R};+,\cdot\rangle$是$\langle R;+,\cdot\rangle$的子环。

证明 由定理 5-12，当且仅当$\langle \tilde{R};+,\cdot\rangle$关于运算$+$满足可逆律时，$\langle \tilde{R},+\rangle$成群。此外，$\langle \tilde{R};+,\cdot\rangle$从$\langle R;+,\cdot\rangle$自动保持了关于运算$+$的可交换性，关于运算$\cdot$的可结合性以及$\cdot$对$+$的可分配性。证完。

于是，若给定一环$\langle R;+,\cdot\rangle$，为了确定R的某一非空子集$\tilde{R}$能否构成$\langle R;+,\cdot\rangle$的子环，只需检验以下条件是否成立：

对于任意的$a,b\in\tilde{R}$，有$a-b\in\tilde{R}$和$ab\in\tilde{R}$。

显然，如果$\langle R;+,\cdot\rangle$是交换环，则其子环也是交换环。

例 1 $\langle R;+,\cdot\rangle$和$\langle\{0\};+,\cdot\rangle$都是$\langle R;+,\cdot\rangle$的子环。

例 2 $\langle I_m;+,\cdot\rangle$，其中$I_m=\{mi|i\in I\}$是$\langle I;+,\cdot\rangle$的一个可换子环（$m$是任一整数）。

例 3 $\langle\{0,2\};\oplus_4,\odot_4\rangle$是$\langle Z_4;\oplus_4,\odot_4\rangle$的可换子环。

定义 6-5 设$V=\langle R;+,\cdot\rangle$是一个环，$\langle D;+,\cdot\rangle$是$V$的子环，如果对于所有的$a\in R$和$d\in D$，$ad$和$da$都属于$D$，则称$\langle D;+,\cdot\rangle$为$V$的**理想子环**，简称为**理想**。若$D$是$R$的真子集，则称理想$\langle D;+,\cdot\rangle$是$V$的**真理想**。

显然，若$D=R$或$D=\{0\}$，则$\langle D;+,\cdot\rangle$是$\langle R;+,\cdot\rangle$的理想。在这种情形下，称$\langle D;+,\cdot\rangle$为**平凡理想**。

例 4 对于任意整数m，环$\langle I;+,\cdot\rangle$的子环$\langle I_m;+,\cdot\rangle$是理想子环。

§6.3 理想与满同态

理想在环论里所占的地位同正规子群在群论里所占的地位类似，下面我们来说明这一点。

设$\langle R;+,\cdot\rangle$和$\langle R';+',\cdot'\rangle$是两个环，$g$是由$R$到$R'$的一个函数。我们知道，若对于所有的$a,b\in R$，有

$$g(a+b)=g(a)+'g(b),\qquad g(a\cdot b)=g(a)\cdot' g(b),$$

则g是由环$\langle R;+,\cdot\rangle$到$\langle R';+',\cdot'\rangle$的同态。

定理 6-4 设$\langle R;+,\cdot\rangle$是一个环，$\langle R';+',\cdot'\rangle$是一个

具有两个二元运算的代数系统，若 g 是由 $\langle R; +, \cdot\rangle$ 到 $\langle R'; +', \cdot'\rangle$ 的满同态，则 $\langle R'; +', \cdot'\rangle$ 也是一个环。

该定理的结论由定理 4-5 直接可得。

设 g 是由环 $\langle R; +, \cdot\rangle$ 到环 $\langle R'; +', \cdot'\rangle$ 的满同态，下面我们证明 g 的核，即 $\langle R'; +', \cdot'\rangle$ 的零元 $0'$ 在 R 中的所有象源的集合，对运算 $+$ 和 $\cdot$ 构成 $\langle R; +, \cdot\rangle$ 的一个理想。

定理 6-5 设 K 是由环 $\langle R; +, \cdot\rangle$ 到环 $\langle R'; +', \cdot'\rangle$ 的满同态 g 的核，则 $\langle K; +, \cdot\rangle$ 是 $\langle R; +, \cdot\rangle$ 的一个理想。

证明 因为 g 是由加法群 $\langle R; +\rangle$ 到加法群 $\langle R'; +'\rangle$ 的满同态，所以 g 的核 K 对运算 $+$ 构成 $\langle R; +\rangle$ 的子群 $\langle K; +\rangle$。又若 $a\in K$，$b\in R$，则

$$g(a\cdot b)=g(a)\cdot' g(b)=0'\cdot' g(b)=0',\ \text{所以}\ a\cdot b\in K.$$

同样地 $g(b\cdot a)=g(b)\cdot' g(a)=g(b)\cdot' 0'=0'$，所以 $b\cdot a\in K$。由上可知 $\langle K; +, \cdot\rangle$ 是 $\langle R; +, \cdot\rangle$ 的一个理想。证完。

于是，由环 $\langle R; +, \cdot\rangle$ 到环 $\langle R'; +', \cdot'\rangle$ 的一个满同态，就得到环 $\langle R; +, \cdot\rangle$ 的一个理想。

反之，假设 $\langle D; +, \cdot\rangle$ 是环 $V=\langle R; +, \cdot\rangle$ 的任一个理想，根据理想的定义可知，$\langle D; +\rangle$ 是 V 的一个正规（加法）子群，因此，在 V 中导致与 $\langle D; +\rangle$ 相关的陪集分划的等价关系 ρ 对于运算 $+$ 满足代换性质（参见第五章习题第 31 题）。现在我们证明 ρ 对于运算 $\cdot$ 也满足代换性质。

事实上，若 $a_1\rho a_2$，$b_1\rho b_2$，则 a_1 与 a_2 属于同一个陪集，设为 c_1+D，b_1 与 b_2 属于同一个陪集，设为 c_2+D。因此存在元素 $d_1, d_2\in D$，使 $a_1=c_1+d_1, a_2=c_1+d_2$，同样也存在元素 $d_3, d_4\in D$，使 $b_1=c_2+d_3, b_2=c_2+d_4$，因而

$$a_1b_1=(c_1+d_1)(c_2+d_3)=c_1c_2+(d_1c_2+c_1d_3+d_1d_3),$$

$$a_2b_2=(c_1+d_2)(c_2+d_4)=c_1c_2+(d_2c_2+c_1d_4+d_2d_4),$$

因为 $\langle D; +, \cdot\rangle$ 是一个理想，所以 d_1c_2，c_1d_3，d_1d_3 都在 D 中，

从而 $d_1c_2+c_1d_2+d_1d_2\in D$，因此 $a_1b_1\in(c_1c_2)+D$，同样地，$a_2b_2\in(c_1c_2)+D$，故有 $(a_1b_1)\rho(a_2b_2)$，即 ρ 对于运算 $\cdot$ 也满足代换性质。于是，ρ 是 $\langle R;+,\cdot\rangle$ 上的同余关系。

因为 ρ 是环 $\langle R;+,\cdot\rangle$ 上的同余关系，所以由定理 4-9(2) 可知，此时必存在一个由 V 到 V/ρ 的满同态。这里 V/ρ 是 V 关于 ρ 的商代数

$$V/\rho=\langle R/\rho;\tilde{+},\tilde{\cdot}\rangle,$$

其中 $R/\rho=\{a+D\mid a\in R\}$ 是 $\langle D;+\rangle$ 的所有陪集的集合。

$$(a_1+D)\tilde{+}(a_2+D)=(a_1+a_2)+D,$$

$$(a_1+D)\tilde{\cdot}(a_2+D)=(a_1a_2)+D.$$

由于 $V=\langle R;+,\cdot\rangle$ 是一个环，由定理 6-4，V/ρ 也是一个环，我们称它为 V 关于 $\langle D;+,\cdot\rangle$ 的**商环**。常用记号 V/D 表示（而不用 V/ρ）。

定理 6-6 若 $\langle D;+,\cdot\rangle$ 是环 $V=\langle R;+,\cdot\rangle$ 的一个理想，则存在一个由环 V 到 V 关于 $\langle D;+,\cdot\rangle$ 的商环 V/D 的满同态。

这一定理说明由环 $V=\langle R;+,\cdot\rangle$ 的任一理想 $\langle D;+,\cdot\rangle$ 可以确定一个由 V 到 V 关于 $\langle D;+,\cdot\rangle$ 的商环的满同态，这个满同态的核是 D。

根据定理 4-9(3)，我们又可直接得到下述结论。

定理 6-7 若 g 是由环 $V_1=\langle R;+,\cdot\rangle$ 到环 $V_2=\langle R';+',\cdot'\rangle$ 的一个满同态，其核是 K，则环 V_2 与环 V_1 关于 $\langle K;+,\cdot\rangle$ 的商环 V_1/K 同构。

例 1 考虑环 $V=\langle I;+,\cdot\rangle$ 和它的理想 $\langle I_5;+,\cdot\rangle$。因为 $\langle I_5;+\rangle$ 是 V 的正规（加法）子群，所以 $\langle I_5;+\rangle$ 的所有陪集构成 I 的分划

$$D=\{I_5,I_5+1,I_5+2,I_5+3,I_5+4\}\qquad(1)$$

于是，V 关于 $\langle I_5;+,\cdot\rangle$ 的商环 $V/I_5=\langle D;\tilde{+},\tilde{\cdot}\rangle$。其中 D 由 (1) 式所定义，运算 $\tilde{+}$ 和 $\tilde{\cdot}$ 定义如下：

$$(I_5+i_1)\tilde{+}(I_5+i_2)=I_5+\mathrm{res}_5(i_1+i_2).$$
$$(I_5+i_1)\tilde{\cdot}(I_5+i_2)=I_5+\mathrm{res}_5(i_1\cdot i_2).$$
其运算表由表 6-1 给出。

表 6-1

$\tilde{+}$	I_5	I_5+1	I_5+2	I_5+3	I_5+4	$\tilde{\cdot}$	I_5	I_5+1	I_5+2	I_5+3	I_5+4
I_5	I_5	I_5+1	I_5+2	I_5+3	I_5+4	I_5	I_5	I_5	I_5	I_5	I_5
I_5+1	I_5+1	I_5+2	I_5+3	I_5+4	I_5	I_5+1	I_5	I_5+1	I_5+2	I_5+3	I_5+4
I_5+2	I_5+2	I_5+3	I_5+4	I_5	I_5+1	I_5+2	I_5	I_5+2	I_5+4	I_5+1	I_5+3
I_5+3	I_5+3	I_5+4	I_5	I_5+1	I_5+2	I_5+3	I_5	I_5+3	I_5+1	I_5+4	I_5+2
I_5+4	I_5+4	I_5	I_5+1	I_5+2	I_5+3	I_5+4	I_5	I_5+4	I_5+3	I_5+2	I_5+1

由运算表可看出 I_5 是商环 V/I_5 的零元。

根据定理 6-6，此时必存在一个由 V 到 V/I_5 的满同态，该满同态由函数

$g: I\to\{I_5, I_5+1, I_5+2, I_5+3, I_5+4\}$ 给出，在这里 $g(i)=I_5+\mathrm{res}_5(i)$。

显然，V/I_5 的零元 I_5 在 I 中所有象源的集合是 I_5，因此满同态 g 的核是 I_5。

我们知道，环 $\langle Z_5; \oplus_5, \odot_5\rangle$ 是环 $V=\langle I; +, \cdot\rangle$ 的满同态象，这一满同态可由 $h: I\to Z_5$ 给出，这里 $h(i)=\mathrm{res}_5(i)$。显然，h 的核是 I_5（0 是 $\langle Z_5; \oplus_5, \odot_5\rangle$ 的零元），因此由定理 6-7，环 $\langle Z_5; \oplus_5, \odot_5\rangle$ 与商环 V/I_5 同构。

事实上，我们可定义函数 $f: Z_5\to D$，使得 $f(z)=I_5+z(z=0, 1, 2, 3, 4)$。显然，$f$ 是一个双射。

又 $\qquad f(z_1\oplus_5 z_2)=f(\mathrm{res}_5(z_1+z_2))=I_5+\mathrm{res}_5(z_1+z_2)$,

$\qquad f(z_1)\tilde{+}f(z_2)=(I_5+z_1)\tilde{+}(I_5+z_2)=I_5+\mathrm{res}_5(z_1+z_2)$,

所以 $\qquad f(z_1\oplus_5 z_2)=f(z_1)\tilde{+}f(z_2)$。

而 $$f(z_1 \odot_5 z_2) = f(\text{res}_5(z_1 \cdot z_2)) = I_5 + \text{res}_5(z_1 \cdot z_2),$$
$$f(z_1) \tilde{\cdot} f(z_2) = (I_5 + z_1) \tilde{\cdot} (I_5 + z_2) = I_5 + \text{res}_5(z_1 \cdot z_2),$$
所以 $$f(z_1 \odot_5 z_2) = f(z_1) \tilde{\cdot} f(z_2).$$
因此，确有环 $\langle Z_5; \oplus_5, \odot_5 \rangle$ 到商环 V/I_5 的同构。

重复上面的论证可知，对任意的正整数 m，都存在一由环 $V = \langle I; +, \cdot \rangle$ 到商环 V/I_m 的满同态。而且环 V/I_m 必与环 $\langle Z_m; \oplus_m, \odot_m \rangle$ 同构。

定义 6-6 设 $\langle D; +, \cdot \rangle$ 是环 $V = \langle R; +, \cdot \rangle$ 的一个理想，如果对于任意的 $a, b \in R$，若 $ab \in D$，便有 $a \in D$ 或 $b \in D$，则称 $\langle D; +, \cdot \rangle$ 是一个**素理想**。

例 2 环 $\langle I; +, \cdot \rangle$ 的理想 $\langle I_5; +, \cdot \rangle$ 是一个素理想。因为，如果 $ab = 5i \in I_5$，则由于 5 是素数，因此或者 a 是 5 的倍数，或者 b 是 5 的倍数，即有 $a \in I_5$ 或 $b \in I_5$。但理想 $\langle I_6; +, \cdot \rangle$ 不是素理想，例如 $2 \cdot 3 = 6 \cdot 1 \in I_6$，但 $2 \notin I_6$，$3 \notin I_6$。

定理 6-8 设 $\langle D; +, \cdot \rangle$ 是具有单位元的交换环 $V = \langle R; +, \cdot \rangle$ 的理想，则当且仅当 $\langle D; +, \cdot \rangle$ 是一个素理想时，V/D 是一个整环。

证明 因为 $\langle D; +, \cdot \rangle$ 是环 V 的理想，所以由定理 6-6，V/D 是 V 的一个满同态象。又由定理 4-5，V/D 必是具有单位元的交换环。

设 $\langle D; +, \cdot \rangle$ 是一个素理想，C_1 和 C_2 是 V/D 的任意两个元素，我们可以写成 $C_1 = D + a$，$C_2 = D + b$ $(a, b \in R)$，从而
$$C_1 \tilde{\cdot} C_2 = (D + a) \tilde{\cdot} (D + b) = D + (ab).$$
若 $C_1 \tilde{\cdot} C_2 = D$，则 $ab \in D$。由 $\langle D; +, \cdot \rangle$ 是素理想，因此有 $a \in D$ 或 $b \in D$，即有 $C_1 = D$ 或 $C_2 = D$。故 V/D 是一无零因子环，从而 V/D 是一个整环。

反之，设 V/D 是一无零因子环，对任意的 $a, b \in R$，令 $C_1 = D + a$，$C_2 = D + b$，则

$$C_1 \widetilde{\cdot} C_2 = (D+a) \widetilde{\cdot} (D+b) = D+(ab).$$

若 $ab \in D$，则 $C_1 \widetilde{\cdot} C_2 = D$，因为 V/D 是无零因子环，因此有 $C_1 = D$ 或 $C_2 = D$，即 $a \in D$ 或 $b \in D$，故 $\langle D; +, \cdot \rangle$ 是一素理想。证完。

定理 6-9 当且仅当 m 是一个素数时，环 $\langle Z_m; \oplus_m, \odot_m \rangle$ 是一个整环。

证明 考虑环 $V = \langle I; +, \cdot \rangle$ 和它的理想 $\langle I_m; +, \cdot \rangle$。当 m 是素数时，对任意的 $ab \in I_m$，可以写成 $ab = mi$，以致 a 和 b 中至少有一个是 m 的倍数。因此对任意的 $ab \in I_m$，有 $a \in I_m$ 或 $b \in I_m$，即当 m 是素数时，$\langle I_m; +, \cdot \rangle$ 是一素理想。由定理 6-8，V/I_m 是一整环，因为 V/I_m 与 $\langle Z_m; \oplus_m, \odot_m \rangle$ 同构，所以 $\langle Z_m; \oplus_m, \odot_m \rangle$ 也是一个整环。

当 m 不是素数时，m 可以写成 $m = ab (1 < a < m, 1 < b < m)$。显然 $a \notin I_m, b \notin I_m$，但 $ab = m \in I_m$，因此 $\langle I_m; +, \cdot \rangle$ 不是素理想，由定理 6-8，V/I_m 不是整环，因此 $\langle Z_m; \oplus_m, \odot_m \rangle$ 也不是整环。证完。

定理 6-9 的结论也可直接由整环的定义推出。这将作为习题，请读者自己证明。

§6.4 域

我们已经在环里给出了逆元的定义，并且知道环的任意一个元素不一定有逆元。现在我们问，在一个环里会不会每一个元素都有逆元呢？在极特殊的情形下这是可能的。

例如，R 只含有一个元素 a，加法和乘法是

$$a + a = a, \qquad aa = a.$$

$\langle R; +, \cdot \rangle$ 显然是一个环。这个环的唯一的元素 a 有一个逆元，就是 a 本身。

但当环 $\langle R; +, \cdot \rangle$ 至少有两个元素的时候情形就不同了。这时，$\langle R; +, \cdot \rangle$ 至少有一个不等于零的元素 a，因此 $0a = 0 \neq$

a。这就是说，0不会是单位元，而且不论a是R中的哪一个元素，总有$0\cdot a=0$。因此环$\langle R;+,\cdot\rangle$中的0不会有逆元。

只含有一个元素的环没有多大的意思，我们不考虑它。我们考虑至少有两个元素的环。这种环的零元不会有逆元我们已经知道，那么，除了零元外，其它的元会不会都有逆元呢？这是可能的。

例1 全体有理数的集合对于通常的加法和乘法来说显然是一个环，这个环的任一元素$q\neq 0$，有逆元$\frac{1}{q}$。

定义6-7 如果环$\langle R;+,\cdot\rangle$是一个含有非零元素（即至少含有两个元素），具有单位元，并且每一个非零元素都有逆元的交换环，则称$\langle R;+,\cdot\rangle$是一个**域**。

例2 $\langle R;+,\cdot\rangle$（这里R是实数集）是一个域。它的单位元是数1，每一元素$r\in R(r\neq 0)$的逆元是$\frac{1}{r}$。$\langle R;+,\cdot\rangle$也是一个整环。

例3 $\langle Z_3;\oplus_3,\odot_3\rangle$是一个域。它的单位元是1，且$1^{-1}=1$，$2^{-1}=2$。$\langle Z_3;\oplus_3,\odot_3\rangle$也是一个整环。

$\langle Z_4;\oplus_4,\odot_4\rangle$不是一个域。它的单位元是1，$1^{-1}=1$，$3^{-1}=3$，但2没有逆元。$\langle Z_4;\oplus_4,\odot_4\rangle$也不是整环。

例4 $\langle I;+,\cdot\rangle$不是一个域。它虽有单位元1，但除了1和-1外，其它非零元素均无逆元。但$\langle I;+,\cdot\rangle$是一个整环。

定理6-10 每一个域都满足消去律（因而是无零因子环）。

证明 设$\langle R;+,\cdot\rangle$是一个域，且$a(\neq 0)$，b，c是R中的元素，若$ab=ac$，则$a^{-1}ab=a^{-1}ac$，因此$b=c$。证完。

由定理6-10立即可得

定理6-11 每一个域都是整环。

这个定理的逆定理不成立。例如整环$\langle I;+,\cdot\rangle$就不是一个域。但当整环是有限的时候，上述定理的逆定理是成立的。

定理6-12 每一个有限整环都是一个域。

证明 设$\langle R;+,\cdot\rangle$是一有限整环，对于任一非零元素

$a\in R$，由消去律可知，如果 $a_i\neq a_j$，则有 $aa_i\neq aa_j$，因此 $a\cdot R=R$。因而必存在某一元素 a_k，使得 $a\cdot a_k=a_k\cdot a=1$。这就是说，每一非零元素 $a\in R$，在 $\langle R;+,\cdot\rangle$ 中都有一个逆元，故 $\langle R;+,\cdot\rangle$ 是一个域。证完。

根据域的定义，若 $\langle R;+,\cdot\rangle$ 是一个域，则 $\langle R;+\rangle$ 是一个加法群，又因为域中没有零因子，因此，对于所有非零元素 $a,b\in R$，$ab\neq 0$。于是，$R-\{0\}$ 对于乘法运算是封闭的。乘法满足结合律，有单位元 $1\in R-\{0\}$，$R-\{0\}$ 中每一元素都有逆元，因此 $\langle R-\{0\};\cdot\rangle$ 构成一乘法群。这样，一个域是由两个群，加法群和乘法群，联合而成的，分配律好象是一座桥将这两个群联系起来。

在域 $\langle R;+,\cdot\rangle$ 中，每一个非零元素 a 都具有两个与之相联系的周期，一个是在加法群中的加法周期，一个是在乘法群中的乘法周期。

例 5 在域 $\langle R;+,\cdot\rangle$ 中（R 是实数集），每一非零实数的加法周期为无限。1 的乘法周期是 1，-1 的乘法周期是 2，此外，其它非零元素的乘法周期为无限。

例 6 在域 $\langle Z_3;\oplus_3,\odot_3\rangle$ 中，1 和 2 的加法周期均是 3。1 的乘法周期是 1，2 的乘法周期是 2。

定理 6-13 设 $\langle R;+,\cdot\rangle$ 是一个域，则 R 中所有非零元素都有相同的加法周期。

证明 设 a，b 是 R 中任意两个非零元素，且 a 有有限的加法周期 n，即 $na=0$，则

$$nb=n(aa^{-1}b)=(na)(a^{-1}b)=0(a^{-1}b)=0.$$

因此，b 也有有限的加法周期，设为 n'，则有 $n'\leqslant n$。类似地

$$n'a=n'(bb^{-1}a)=(n'b)(b^{-1}a)=0(b^{-1}a)=0,$$

因此又有 $n\leqslant n'$。

由上可知，$n=n'$。这说明 R 中所有非零元素都有相同的加法周期。证完。

R中所有非零元素所具有的同一加法周期，称为域$\langle R;+,\cdot\rangle$的**特征**。

例如，实数域$\langle R;+,\cdot\rangle$的特征为无限，域$\langle Z_3;\oplus_3,\odot_3\rangle$的特征是3。

定理6-14 每一个有限域的特征是一个素数。

证明 设$\langle R;+,\cdot\rangle$是特征为r的有限域，由定理5-11，r是一有限数，假设r不是素数，则$r=mn$，其中$m<r,n<r$。因此

$$0=r1=(mn)1=m(n1).$$

因为$n1\in R$的加法周期也为r，所以应有$r\leqslant m$，这与$m<r$矛盾。因此r必为素数。证完。

习　　题

1. 设R是实数集，加法$+$是普通的加法，但乘法$\times$是

$$a\times b=|a|b,$$

$\langle R;+,\times\rangle$是否成环？

2. 设$\langle R;+,\cdot\rangle$是环，又设a,b和c是R中的任意元素，试证明：

(1) 若$ab=ba$，则$a(-b)=(-b)a$，$a(nb)=(nb)a$（n为整数）以及$ab^{-1}=b^{-1}a$；

(2) 若$ab=ba$和$ac=ca$，则$a(b+c)=(b+c)a$，$a(bc)=(bc)a$。

3. 设$\langle R;+,\cdot\rangle$是一有单位元的环，定义R的一个子集$\bar{R}$为

$$\bar{R}=\{a\mid a^{-1}\text{也在}R\text{中}\},$$

试证$\langle\bar{R};\cdot\rangle$是一个群。

4. 设R是所有有理数对(a_1,a_2)的集合，它们的结合法是

$$(a_1,a_2)+(b_1,b_2)=(a_1+b_1,a_2+b_2),$$

$$(a_1,a_2)\cdot(b_1,b_2)=(a_1b_1,a_2b_2),$$

那么$\langle R;+,\cdot\rangle$是否成环？它是否有零因子？是否有单位元？哪些元素有逆元？

5. 设$\langle R;+,\cdot\rangle$是一个环，且对于所有的$a\in R$，有$a^2=a$（这样的环称为布尔环）：

(1) 证明对所有的$a\in R$，有$a+a=0$；

(2) 证明$\langle R;+,\cdot\rangle$是个交换环；

(3) 证明：若$\#R>2$，则$\langle R;+,\cdot\rangle$不可能是整环。

6. 证明$\langle I;\oplus,\odot\rangle$是一具有单位元的交换环。这里运算$\oplus$和$\odot$定义如下：

$$a\oplus b=a+b-1,\ a\odot b=a+b-ab.$$

7. 给定环$\langle R;+,\cdot\rangle$。试证明：对于任意的$a,b\in R$，有

$$(a+b)^2=a^2+ab+ba+b^2.$$

8. 找出环$\langle Z_6;\oplus_6,\odot_6\rangle$的所有子环和理想。

9. 试证明：如果$\langle D_1;+,\cdot\rangle$和$\langle D_2;+,\cdot\rangle$是环$V=\langle R;+,\cdot\rangle$的理想，则

(1) $\langle D_1+D_2;+,\cdot\rangle$也是$V$的理想，

$(D_1+D_2=\{d_{1i}+d_{2j}\mid d_{1i}\in D_1,d_{2j}\in D_2\})$；

(2) $\langle D_1\cap D_2;+,\cdot\rangle$也是$V$的理想。

10. 设g是由环$V_1=\langle R;+,\cdot\rangle$到环$V_2=\langle R';+',\cdot'\rangle$的满同态。试证明：当且仅当$g$的核$K=\{0\}$时，$g$是由环$V_1$到$V_2$的同构。

11. 构造一个具有三个元素的域。

12. 代数系统$\langle R;+,\cdot\rangle$定义为：

+	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

·	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	c	d	b
d	a	d	b	c

(1) 证明$\langle R;+,\cdot\rangle$是一个域；

(2) 求解$\langle R;+,\cdot\rangle$中的方程组

$$\begin{cases}x+cy=a\\cx+y=b.\end{cases}$$

13. 试证明：当且仅当p为素数时，环$\langle Z_p;\oplus_p,\odot_p\rangle$是一个域。并求出该域的特征。

14. 试证明两个域的积代数一定不是域。

15. 设$\langle R;+,\cdot\rangle$是一个具有四个元素的域。试证明：

(1) $\langle R;+,\cdot\rangle$的特征是2；

(2) R中不为0和1的两个元素都适合方程$x^2=x+1$。

16. 假设环$\langle R;+,\cdot\rangle$对于加法成为一个循环群。证明$\langle R;+,\cdot\rangle$是交换环。

17. 证明由所有实数$a+b\sqrt{2}$（a,b是整数）组成的集合对于通常的加法和乘法构成一个整环。

18. 设g是由环$\langle R;+,\cdot\rangle$到环$\langle R';+',\cdot'\rangle$的满同态。试证明：

(1) 若$\langle\bar{R};+,\cdot\rangle$是环$\langle R;+,\cdot\rangle$的子环，则$\bar{R}$的象$\bar{R}'$对于运算$+'$和$\cdot'$也构成$\langle R';+',\cdot'\rangle$的子环；

(2) 若$\langle K;+,\cdot\rangle$是环$\langle R;+,\cdot\rangle$的理想，则K的象K'对于运算$+'$和$\cdot'$也构成$\langle R';+',\cdot'\rangle$的理想；

(3) 若$\langle\bar{R}';+',\cdot'\rangle$是环$\langle R';+',\cdot'\rangle$的子环，则$\bar{R}'$的象源$\bar{R}$对于运算$+$和$\cdot$也构成$\langle R;+,\cdot\rangle$的子环；

(4) 若$\langle K';+',\cdot'\rangle$是环$\langle R';+',\cdot'\rangle$的理想，则$K'$的象源$K$对于运算$+$和$\cdot$也构成$\langle R;+,\cdot\rangle$的理想。

第七章　格和布尔代数

本章介绍代数系统格，其结构是以第二章所介绍的偏序关系为基础。我们将推导格的性质，并给出格的各种实例。附加一些条件后，格就变成布尔代数。我们将证明，每一个有限布尔代数都同构于某一个集合代数。从而，每一个有限布尔代数的基数都是 2 的幂。我们还将证明，每一个基数为 2^r 的布尔代数与 r 个基数为 2 的布尔代数的积代数同构。最后讨论布尔函数及其标准形式。

格的概念在有限自动机的很多方面都是重要的。布尔代数可直接用于开关理论和逻辑设计。因此，对于计算机科学来说，格与布尔代数是两个很重要的代数系统。

§7.1 偏序集

在第二章里我们曾将集合 L 上的自反、反对称且可传递的关系称为集合 L 上的偏序关系，并用记号"$\leqslant$"来表示。今将集合 L 和 L 上的偏序关系 $\leqslant$ 一起称为一个**偏序集**，用 $\langle L;\leqslant\rangle$ 来表示。由于 $\leqslant$ 和它的逆 $\geqslant$ 都是 L 上的偏序关系，因此，对于偏序集 $\langle L;\leqslant\rangle$ 中所有的元素 $l_1,l_2,l_3\in L$，有

$$l_1\leqslant l_1. \quad (7\text{-}1)$$

若　$l_1\leqslant l_2$，$l_2\leqslant l_1$，　则有 $l_1=l_2$。　(7-2)

若　$l_1\leqslant l_2$，$l_2\leqslant l_3$，　则有 $l_1\leqslant l_3$。　(7-3)

$$l_1\geqslant l_1. \quad (7\text{-}1')$$

若　$l_1\geqslant l_2$，$l_2\geqslant l_1$，　则有 $l_1=l_2$。　(7-2′)

若　$l_1\geqslant l_2$，$l_2\geqslant l_3$，　则有 $l_1\geqslant l_3$。　(7-3′)

符号“$\leqslant$”通常读作“小于或者等于”。我们说 l_1 小于或者等于 l_2，意思就是 $l_1 \leqslant l_2$。我们说 $l_1 < l_2$，意思是 $l_1 \leqslant l_2$，但 $l_1 \neq l_2$。符号“$\geqslant$”通常读作“大于或者等于”。$l_2 \geqslant l_1$ 等价于 $l_1 \leqslant l_2$。

定义 7-1 设 l_1 和 l_2 是偏序集 $\langle L; \leqslant \rangle$ 中的两个元素，元素 $a \in L$，如果满足 $a \leqslant l_1$，$a \leqslant l_2$，则称 a 为 l_1 和 l_2 的**下界**。如果元素 a 是 l_1 和 l_2 的下界，且对于任意的 $a' \in L$，若 a' 是 l_1 和 l_2 的下界，便有 $a' \leqslant a$，则称 a 是 l_1 和 l_2 的**最大下界**，简记为 glb。

定义 7-2 设 l_1 和 l_2 是偏序集 $\langle L; \leqslant \rangle$ 中的两个元素，元素 $b \in L$，如果满足 $l_1 \leqslant b, l_2 \leqslant b$，则称 b 为 l_1 和 l_2 的**上界**。如果元素 b 是 l_1 和 l_2 的上界，且对于任意的 $b' \in L$，若 b' 是 l_1 和 l_2 的上界，便有 $b \leqslant b'$，则称 b 是 l_1 和 l_2 的**最小上界**，简记为 lub。

定理 7-1 设 l_1 和 l_2 是偏序集 $\langle L; \leqslant \rangle$ 的两个元素，如果 l_1 和 l_2 有 glb，则 glb 是唯一的。如果 l_1 和 l_2 有 lub，则 lub 是唯一的。

证明 设 a_1 和 a_2 都是 l_1 和 l_2 的 glb。由定义 7-1，有

$$a_1 \leqslant l_1, \quad a_1 \leqslant l_2, \quad a_2 \leqslant l_1, \quad a_2 \leqslant l_2,$$

且

$$a_2 \leqslant a_1, \quad a_1 \leqslant a_2.$$

由 $\leqslant$ 的反对称性得 $$a_1 = a_2.$$

类似的方法可证明 lub 的唯一性。证完。

在 $\langle L; \leqslant \rangle$ 的次序图中，l_1 和 l_2 有最大下界这一事实反映为：从结点 l_1 和 l_2 出发，经过向下的路径至少可以共同到达次序图的一个结点，这些结点中最上面的那一个就代表 l_1 和 l_2 的最大下界。同样，l_1 和 l_2 有最小上界这一事实反映为：从结点 l_1 和 l_2 出发，经过向上的路径至少可以共同到达次序图的一个结点，这些结点中最下面的那一个就代表 l_1 和 l_2 的最小上界。

例 1 设有集合 $U = \{a, b, c\}$，U 的幂集 2^U 上的包含关系 $\subseteq$ 是一偏序关系。

图7-1给出了$\langle 2^S;\subseteq\rangle$的次序图。由图7-1可看出$\{a,b,c\}$是$\{a,b\}$和$\{b,c\}$的上界，也是$\{a,b\}$和$\{b,c\}$的最小上界。$\{b\}$和$\phi$是$\{a,b\}$和$\{b,c\}$的下界，其中$\{b\}$是它们的最大下界。$\{a,b,c\}$和$\{a,b\}$是$\{a,b\}$和$\{b\}$的上界，其中$\{a,b\}$是最小上界。

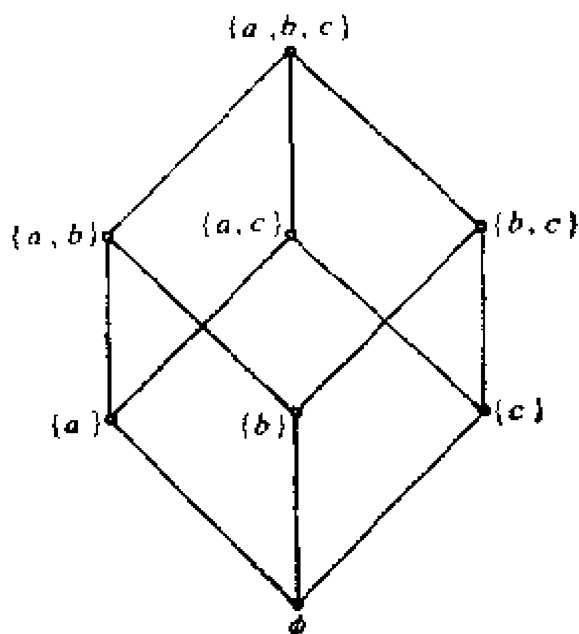


图7-1

定义7-3 设$\langle L;\leqslant\rangle$是一偏序集，

(1) 如果对于所有的元素$l\in L$，有$a\leqslant l$，则称元素$a\in L$是**最小元素**。

(2) 如果对于所有的元素$l\in L$，有$l\leqslant b$，则称元素$b\in L$是**最大元素**。

定理7-2 如果偏序集$\langle L;\leqslant\rangle$有最小元素，则最小元素是唯一的。如果$\langle L;\leqslant\rangle$有最大元素，则最大元素是唯一的。

证明 设a_1和a_2都是$\langle L;\leqslant\rangle$的最小元素；$b_1$和$b_2$都是$\langle L;\leqslant\rangle$的最大元素。则由定义7-3，有$a_1\leqslant a_2, a_2\leqslant a_1$，$b_1\leqslant b_2$，$b_2\leqslant b_1$。由反对称性，得$a_1=a_2$，$b_1=b_2$。证完。

例2 §2.7例6给出了偏序集$\langle J;|\rangle$及其次序图(图2-6)，由图中可看出，它没有最大元素，也没有最小元素；2和3没有下界，因而没有最大下界；8和12没有上界，因而也没有最小上界。

§7.2 格及其性质

从上一节的例2我们知道，对任意一个偏序集来说，其中的每一对元素不一定都有最大下界或最小上界。这一节我们讨论其

中每一对元素都有最大下界和最小上界的偏序集，并将这种偏序集称作是"格"。

定义 7-4 **格**是一个偏序集$\langle L;\leqslant\rangle$，其中每一对元素$l_1$，$l_2\in L$均存在最大下界和最小上界。

我们通常将元素l_1和l_2的最大下界和最小上界分别用$l_1\wedge l_2$和$l_1\vee l_2$来表示。即$l_1\wedge l_2=\mathrm{glb}(l_1,l_2)$，$l_1\vee l_2=\mathrm{lub}(l_1,l_2)$。由于每一对元素的最大下界和最小上界是唯一的，因此$\wedge$和$\vee$均可看作是集合L上的二元运算。我们将运算$\wedge$和$\vee$分别称为**交**和**并**。

根据glb和lub的定义，在格$\langle L;\leqslant\rangle$中，对于所有的元素$l_1$，$l_2,l_3\in L$，有

$$l_1\wedge l_2\leqslant l_1,\quad l_1\wedge l_2\leqslant l_2. \tag{7-4}$$

若 $l_3\leqslant l_1$，$l_3\leqslant l_2$， 则$l_3\leqslant l_1\wedge l_2$。 **(7-5)**

$$l_1\vee l_2\geqslant l_1,\quad l_1\vee l_2\geqslant l_2. \tag{7-4'}$$

若 $l_3\geqslant l_1$，$l_3\geqslant l_2$， 则$l_3\geqslant l_1\vee l_2$。 **(7-5')**

例 1 全集合U的幂集2^U和定义在其上的包含关系构成偏序集$\langle 2^U;\subseteq\rangle$。对于任意子集$S_1,S_2\subseteq U$，有$S_1\subseteq S_1\cup S_2$，$S_2\subseteq S_1\cup S_2$，并且若有子集$S\subseteq U$，使得$S_1\subseteq S$，$S_2\subseteq S$，则必有$S_1\cup S_2\subseteq S$。因此，幂集$2^U$中任意子集对$(S_1,S_2)$有lub，且$\mathrm{lub}(S_1,S_2)=S_1\cup S_2$。同样，任意子集对$(S_1,S_2)$有glb，且$\mathrm{glb}(S_1,S_2)=S_1\cap S_2$。

于是，$\langle 2^U;\subseteq\rangle$是一个格。

例 2 正整数集N上的整除关系$|$是一个偏序关系。对于任意两个正整数n_1和n_2，既存在lub，又存在glb。

$\mathrm{lub}(n_1,n_2)=\mathrm{lcm}(n_1,n_2)$ （n_1和n_2的最小公倍数），

$\mathrm{glb}(n_1,n_2)=\gcd(n_1,n_2)$ （n_1和n_2的最大公约数）。

因此，$\langle N;|\rangle$是一个格。

例 3 设n是一正整数，S_n是n的所有正因子的集合。例如

若 $n=6$， 则$S_6=\{1,2,3,6\}$；

若 $n=24$， 则$S_{24}=\{1,2,3,4,6,8,12,24\}$。

设$|$是整除关系，显然，对于任意正整数n，$|$是S_n上的偏序关系。

图7-2的(a)、(b)、(c)和(d)分别给出了偏序集$\langle S_6;|\rangle$、$\langle S_8;|\rangle$、$\langle S_{24};|\rangle$和$\langle S_{30};|\rangle$的次序图。由图中可看出，它们都是格。

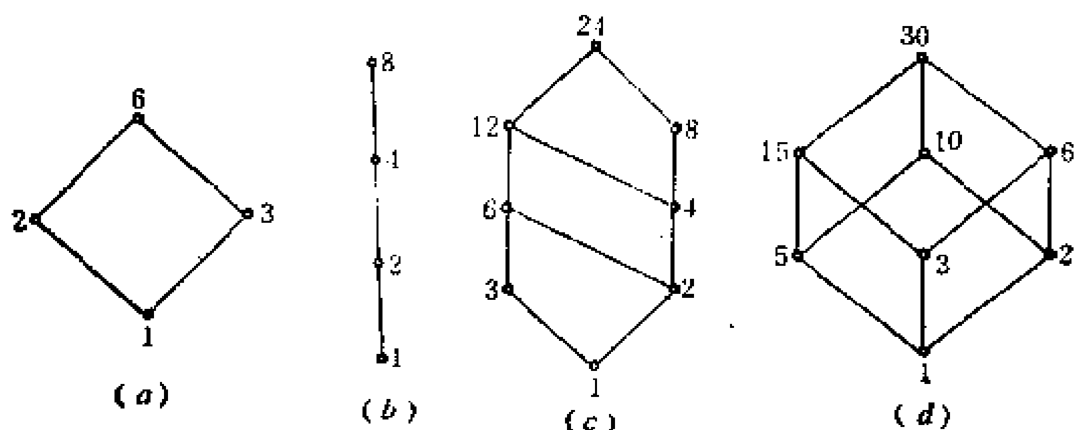


图7-2

显然，并不是每一个偏序集都是格。例如上一节例2的偏序集$\langle\{2,3,4,6,8,12,36,60\};|\rangle$就不是一个格。图7-3也给出了几个不是格的偏序集的例子。

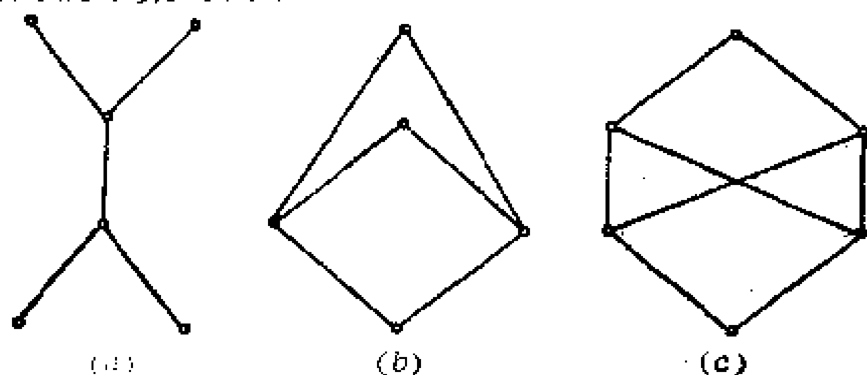


图 7-3

现在我们来看格具有什么性质。

定理 7-3 如果l_1和l_2是格$\langle L;\leqslant\rangle$的元素，则

$$(l_1\vee l_2=l_2)\Leftrightarrow(l_1\wedge l_2=l_1)\Leftrightarrow(l_1\leqslant l_2).$$

证明 设$l_1\vee l_2=l_2$，由(7-4′)有$l_1\leqslant l_2$，又由自反性$l_1\leqslant l_1$，于是由(7-5)，有$l_1\leqslant l_1\wedge l_2$。而由(7-4)，有$l_1\wedge l_2\leqslant l_1$，因此，由反对称性，得$l_1\wedge l_2=l_1$。

设 $l_1 \wedge l_2 = l_1$，则由(7-4)，有 $l_1 \leqslant l_2$。

设 $l_1 \leqslant l_2$，由自反性 $l_2 \leqslant l_2$，因而由（7-5′），有 $l_2 \geqslant l_1 \vee l_2$，又由(7-4′)，有 $l_1 \vee l_2 \geqslant l_2$，故由反对称性，得 $l_1 \vee l_2 = l_2$。

这就证明了 $(l_1 \vee l_2 = l_2) \Leftrightarrow (l_1 \wedge l_2 = l_1) \Leftrightarrow (l_1 \leqslant l_2)$。证完。

一个含有格的元素和符号 $=, \leqslant, \geqslant, \vee, \wedge$ 的关系式的**对偶**，是指用 $\geqslant, \leqslant, \vee$ 和 $\wedge$ 分别代替此关系式中的 $\leqslant, \geqslant, \wedge$ 和 $\vee$ 所得的关系式. 关系式 P 的对偶表示为 P^D。显然，若 P^D 是 P 的对偶，则 P 也是 P^D 的对偶。因此，P 与 P^D 互为对偶。

容易看出，前面列出的代表格的定义的十个基本关系式中，(7-1′)，(7-2′)，(7-3′)，(7-4′)，(7-5′)分别是(7-1)，(7-2)，(7-3)，(7-4)，(7-5)的对偶. 由此可见，在格的任一由这些基本关系式所导出的关系式中，同时交换 $\leqslant$ 和 $\geqslant$ 以及 $\vee$ 和 $\wedge$ 所得到的关系式也可以从这些基本关系式的对偶导出。因此，为了证明交换后所得到的关系式，我们只需要在原关系式的证明中作上述代换就行了。于是，对于格中的每一条定理都存在着一条相对偶的定理. 也就是说，在格中我们有**对偶原理**：对于格 $\langle L; \leqslant \rangle$ 上的任一真命题，其对偶亦为真。

下面每一条定理都包含一对相对偶的恒等式，我们除对交换律同时给出相对偶的证明过程外，其它将不再写出这种成对的证明。

定理 7-4 （交换律）

对于任意的 $l_1, l_2 \in L$，有

(a) $l_1 \vee l_2 = l_2 \vee l_1$；(b) $l_1 \wedge l_2 = l_2 \wedge l_1$。

证明 (a) 由(7-4′)有 $l_1 \vee l_2 \geqslant l_2$，$l_1 \vee l_2 \geqslant l_1$，则由(7-5′)有 $l_1 \vee l_2 \geqslant l_2 \vee l_1$。类似地，由(7-4′)有 $l_2 \vee l_1 \geqslant l_1$，$l_2 \vee l_1 \geqslant l_2$，则由(7-5′)有 $l_2 \vee l_1 \geqslant l_1 \vee l_2$。于是由反对称性，得 $l_1 \vee l_2 = l_2 \vee l_1$。

(b) 由(7-4)有 $l_1 \wedge l_2 \leqslant l_2$，$l_1 \wedge l_2 \leqslant l_1$，则由(7-5)有 $l_1 \wedge l_2 \leqslant l_2 \wedge l_1$。类似地，由(7-4)有 $l_2 \wedge l_1 \leqslant l_1$，$l_2 \wedge l_1 \leqslant l_2$，则由(7-5)有 $l_2 \wedge l_1 \leqslant l_1 \wedge l_2$。于是由反对称性，得 $l_1 \wedge l_2 = l_2 \wedge l_1$。证完。

定理 7-5 （结合律）

对于任意的$l_1,l_2,l_3\in L$，有

(a) $l_1\vee(l_2\vee l_3)=(l_1\vee l_2)\vee l_3$，

(b) $l_1\wedge(l_2\wedge l_3)=(l_1\wedge l_2)\wedge l_3$。

证明 (a) 设$a=l_1\vee(l_2\vee l_3)$，$a'=(l_1\vee l_2)\vee l_3$，由(7-4′)有$a\geqslant l_1,a\geqslant l_2\vee l_3$，再由（7-4′）和传递性，有$a\geqslant l_2,a\geqslant l_3$，于是有$a\geqslant l_1,a\geqslant l_2$，由(7-5′)有$a\geqslant l_1\vee l_2$，又因为$a\geqslant l_3$，所以由(7-5′)有$a\geqslant(l_1\vee l_2)\vee l_3$，即$a\geqslant a'$。

类似地可证明$a'\geqslant a$。

最后由反对称性，得$a=a'$。证完。

由于有结合律，因此我们常将$l_1\vee(l_2\vee l_3)=(l_1\vee l_2)\vee l_3$写成$l_1\vee l_2\vee l_3$；将$l_1\wedge(l_2\wedge l_3)=(l_1\wedge l_2)\wedge l_3$写成$l_1\wedge l_2\wedge l_3$。利用归纳法可以证明，对于任意$n$个元素$l_1,l_2,\cdots,l_n\in L$，结合律也是成立的，即不加括号的表达式

$l_1\vee l_2\vee\cdots\vee l_n$(简记成$\bigvee\limits_{i=1}^{n}l_i$)和$l_1\wedge l_2\wedge\cdots\wedge l_n$(简记成$\bigwedge\limits_{i=1}^{n}l_i$)分别唯一地表示$L$中的一个元素。

我们推广最大下界和最小上界到集合L的任意一个子集H。

设$\langle L;\leqslant\rangle$是一偏序集，$H$是$L$的一个子集，如果元素$a\in L$，对于所有的$h\in H$，有$a\leqslant h$，则称$a$是子集$H$的**下界**。若$a$是$H$的下界，且对于任意的$a'\in L$，若$a'$是$H$的下界，便有$a'\leqslant a$，则称$a$是$H$的**最大下界**。如果元素$b\in L$，对于所有的$h\in H$，有$h\leqslant b$，则称$b$是$H$的**上界**。如果$b$是$H$的上界，且对于任意的$b'\in L$，若$b'$是$H$的上界，便有$b\leqslant b'$，则称$b$是$H$的**最小上界**。

容易证明，在格$\langle L;\leqslant\rangle$中，$l_1\wedge l_2\wedge\cdots\wedge l_n$就是元素$l_1,l_2,\cdots,l_n$的最大下界；$l_1\vee l_2\vee\cdots\vee l_n$就是$l_1,l_2,\cdots,l_n$的最小上界。即

若令$a=l_1\wedge l_2\wedge\cdots\wedge l_n$，则$a\leqslant l_1,a\leqslant l_2,\cdots,a\leqslant l_n$。 (7-6)

若$a'\leqslant l_1,a'\leqslant l_2,\cdots,a'\leqslant l_n$，则$a'\leqslant a$。 (7-7)

若令$b=l_1\vee l_2\vee\cdots\vee l_n$，则$b\geqslant l_1,b\geqslant l_2,\cdots,b\geqslant l_n$。 (7-6′)

若$b'\geqslant l_1,b'\geqslant l_2,\cdots,b'\geqslant l_n$，则$b'\geqslant b$。 (7-7′)

下面用对元素个数 n 进行归纳的方法给出 (7-6) 和 (7-7) 式的证明。

当 $n=1$ 和 $n=2$ 时，(7-6) 和 (7-7) 显然成立。

假设 $l_1 \wedge l_2 \wedge \cdots \wedge l_k$ 是 $l_1, l_2, \cdots, l_k$ 的最大下界。由结合律可知 $l_1 \wedge l_2 \wedge \cdots \wedge l_k \wedge l_{k+1} = (l_1 \wedge l_2 \wedge \cdots \wedge l_k) \wedge l_{k+1} = a$（令其为 a）。由 (7-4) 有 $a \leqslant l_1 \wedge l_2 \wedge \cdots \wedge l_k, a \leqslant l_{k+1}$。由归纳假设 $l_1 \wedge l_2 \wedge \cdots \wedge l_k \leqslant l_i (i=1,2,\cdots,k)$，因此由传递性，有 $a \leqslant l_1, a \leqslant l_2, \cdots, a \leqslant l_k$，又因为 $a \leqslant l_{k+1}$ 所以 $l_1 \wedge l_2 \wedge \cdots \wedge l_k \wedge l_{k+1}$ 是 $l_1, l_2, \cdots, l_{k+1}$ 的下界。又若有 $a' \in L$ 且 $a' \leqslant l_1, a' \leqslant l_2, \cdots, a' \leqslant l_{k+1}$，则由归纳假设有 $a' \leqslant l_1 \wedge l_2 \wedge \cdots \wedge l_k$，又因为 $a' \leqslant l_{k+1}$，则由 (7-5) 有 $a' \leqslant (l_1 \wedge l_2 \wedge \cdots \wedge l_k) \wedge l_{k+1}$，所以 $l_1 \wedge l_2 \wedge \cdots \wedge l_k \wedge l_{k+1}$ 是 $l_1, l_2, \cdots, l_{k+1}$ 的最大下界。以上即说明 (7-6) 和 (7-7) 式成立。证完。

根据对偶原理 (7-6′) 和 (7-7′) 亦成立。

定理 7-6 （等幂律）

对于任意的 $l \in L$，有

(a) $l \vee l = l$，(b) $l \wedge l = l$。

证明 (a) 由 (7-4′) 有 $l \vee l \geqslant l$，

而由 (7-1′) 有 $l \geqslant l$，

因此又由 (7-5′) 有 $l \geqslant l \vee l$，

于是由 (7-2′) 得 $l \vee l = l$。证完。

定理 7-7 （吸收律）

对于任意的 $l_1, l_2 \in L$，有

(a) $l_1 \vee (l_1 \wedge l_2) = l_1$，(b) $l_1 \wedge (l_1 \vee l_2) = l_1$。

证明 (b) 由 (7-4) 有 $l_1 \wedge (l_1 \vee l_2) \leqslant l_1$。但由自反性 $l_1 \leqslant l_1$，由 (7-4′) $l_1 \leqslant l_1 \vee l_2$，因此由 (7-5) 有 $l_1 \leqslant l_1 \wedge (l_1 \vee l_2)$。由反对称性，得 $l_1 \wedge (l_1 \vee l_2) = l_1$。证完。

格 $\langle L; \leqslant \rangle$ 除具有上述主要性质外，格中的元素还有如下一些关系。

定理 7-8 对于任意的 $l_1, l_2, l_3 \in L$，若 $l_2 \leqslant l_3$，则 $l_1 \wedge l_2 \leqslant l_1 \wedge l_3$，$l_1 \vee l_2 \leqslant l_1 \vee l_3$。

证明 因为 $l_2 \leqslant l_3$，根据定理 7-3，便有 $l_2 \wedge l_3 = l_2$，于是 $(l_1 \wedge l_2) \wedge (l_1 \wedge l_3) = (l_1 \wedge l_1) \wedge (l_2 \wedge l_3) = l_1 \wedge (l_2 \wedge l_3) = l_1 \wedge l_2$。因此

$$l_1 \wedge l_2 \leqslant l_1 \wedge l_3.$$

类似地可证明 $l_1 \vee l_2 \leqslant l_1 \vee l_3$。证完。

定理 7-9 对于任意的 $l_1, l_2, l_3 \in L$，有下列分配不等式成立：

(a) $l_1 \vee (l_2 \wedge l_3) \leqslant (l_1 \vee l_2) \wedge (l_1 \vee l_3)$，

(b) $l_1 \wedge (l_2 \vee l_3) \geqslant (l_1 \wedge l_2) \vee (l_1 \wedge l_3)$。

其证明请读者自己给出。

§7.3 格是一种代数系统

由上一节我们已知道，如果 $\langle L; \leqslant \rangle$ 是一个格，则 L 中任一元素对 l_1 和 l_2 都有唯一的 glb 和 lub，若我们分别采用 $l_1 \wedge l_2$ 和 $l_1 \vee l_2$ 来表示它们，则"$\wedge$"和"$\vee$"可看作是集合 L 上的两个二元运算，它们满足交换律、结合律、等幂律和吸收律。现在我们要说明这一结论的逆也是成立的，即若在集合 L 上定义了两个二元运算，且这两个运算满足以上四条定律，则 L 上必存在一个偏序关系 $\leqslant$，使得 $\langle L; \leqslant \rangle$ 成为一个格。

定理 7-10 设 L 是一定义了两个二元运算 $\vee$ 和 $\wedge$ 的集合，这两个运算都满足交换律、结合律和吸收律，则必存在一 L 上的偏序关系，使得在此偏序关系下，对于每一对元素 $l_1, l_2 \in L$，$l_1 \vee l_2$ 就是 l_1 和 l_2 的 lub，$l_1 \wedge l_2$ 就是 l_1 和 l_2 的 glb。

在定理中没有列出等幂律。这是因为在定理的条件下，等幂律是自然满足的。事实上，由吸收律可推出等幂律，即对于任意的 $l \in L$，

$$l \vee l = l \vee [l \wedge (l \vee l)] = l.$$

用同样的方法或由对偶原理可以证明 $l\wedge l=l$。因此在下面的证明中，我们可以认为等幂律也是成立的。

证明 定义 L 上的关系 $\leqslant$：对于任意的 l_1，$l_2\in L$，

当且仅当 $l_1\vee l_2=l_1$ 时，有 $l_2\leqslant l_1$。 (7-8)

由等幂律，对于任一 $l\in L$，有 $l\vee l=l$，所以 $l\leqslant l$，因此 $\leqslant$ 是自反的。

设 $l_1\leqslant l_2$ 且 $l_2\leqslant l_1$，则由 (7-8) 有 $l_2\vee l_1=l_2$ 且 $l_1\vee l_2=l_1$，由交换律可得 $l_1=l_2$，因此 $\leqslant$ 是反对称的。

设 $l_1\leqslant l_2$ 且 $l_2\leqslant l_3$，则由 (7-8) $l_2\vee l_1=l_2$，$l_3\vee l_2=l_3$，由结合律可得

$$l_3\vee l_1=(l_3\vee l_2)\vee l_1=l_3\vee(l_2\vee l_1)=l_3\vee l_2=l_3,$$

于是又由(7-8)有 $l_1\leqslant l_3$，即 $\leqslant$ 是可传递的。

由以上可知，$\leqslant$ 是 L 上的一个偏序关系。

对于任意的 $l_1,l_2\in L$，由交换律、结合律和等幂律，有

$$(l_1\vee l_2)\vee l_1=l_1\vee(l_1\vee l_2)=(l_1\vee l_1)\vee l_2=l_1\vee l_2,$$

因此，由 (7-8) 有 $l_1\vee l_2\geqslant l_1$。类似地可证明，对于任意的 $l_1,l_2\in L$，有 $l_1\vee l_2\geqslant l_2$。又由 (7-8)，若 $l_3\geqslant l_1$，$l_3\geqslant l_2$，则 $l_3\vee l_1=l_3$，$l_3\vee l_2=l_3$，因此

$$l_3\vee(l_1\vee l_2)=(l_3\vee l_1)\vee l_2=l_3\vee l_2=l_3,$$

即 $l_3\geqslant l_1\vee l_2$。故 $l_1\vee l_2=\mathrm{lub}(l_1,l_2)$。

若 $l_1\vee l_2=l_1$，则 $l_2\wedge(l_1\vee l_2)=l_2\wedge l_1$。于是，由吸收律有 $l_1\wedge l_2=l_2$。反之，若 $l_1\wedge l_2=l_2$，则 $l_1\vee(l_1\wedge l_2)=l_1\vee l_2$。于是，由吸收律有 $l_1\vee l_2=l_1$。因此

$$(l_1\wedge l_2=l_2)\Longleftrightarrow(l_1\vee l_2=l_1).$$

于是关系 $\leqslant$ 又可定义为：对于所有的 $l_1,l_2\in L$，

当且仅当 $l_1\wedge l_2=l_2$ 时，有 $l_2\leqslant l_1$。 (7-9)

运用上面论证过程的对偶及借助 (7-9) 可得 $l_1\wedge l_2=\mathrm{glb}(l_1,l_2)$。证完。

综合本节和上节的结论，我们可以给出与定义 7-4 等价的格的另一种定义，即将格定义为一种代数系统。

定义 7-5 设 $\langle L; \vee, \wedge\rangle$ 是一个代数系统，$\vee$ 和 $\wedge$ 是 L 上的两个二元运算，如果这两个运算满足交换律、结合律和吸收律，则称 $\langle L; \vee, \wedge\rangle$ 是一个格。

§7.4 分配格和有补格

由定理7-9，我们知道格满足分配不等式。但任给一个格 $\langle L; \vee, \wedge\rangle$，其运算 $\vee$ 与 $\wedge$ 不一定能满足分配律。

定义 7-6 设 $\langle L; \vee, \wedge\rangle$ 是一个格，若对于任意的 $l_1, l_2, l_3 \in L$，有

$$l_1 \wedge (l_2 \vee l_3) = (l_1 \wedge l_2) \vee (l_1 \wedge l_3),$$

$$l_1 \vee (l_2 \wedge l_3) = (l_1 \vee l_2) \wedge (l_1 \vee l_3),$$

则称 $\langle L; \vee, \wedge\rangle$ 为**分配格**。

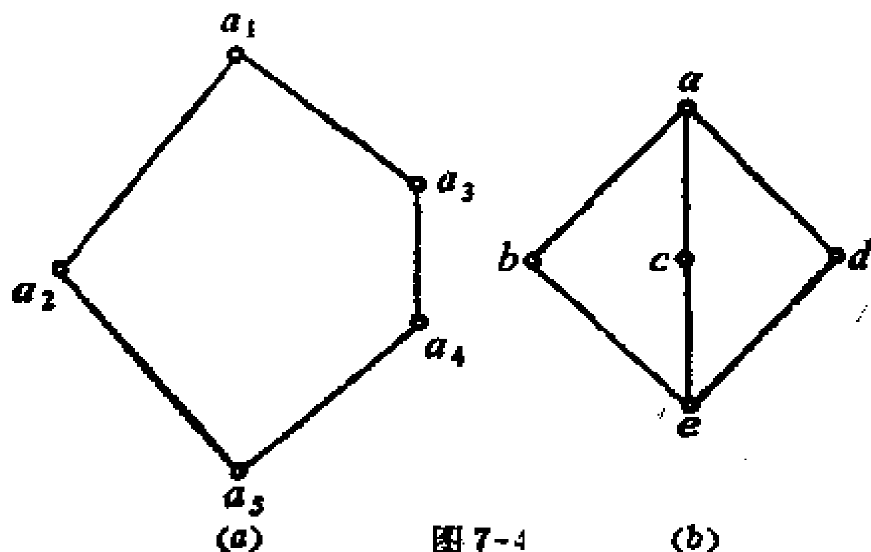
例 1 全集合 U 的幂集 2^U 与其上所定义的并和交运算所组成的格 $\langle 2^U; \cup, \cap\rangle$ 是一个分配格。

图 7-4 所给出的两个格都不是分配格。因为在图7-4(a)中

$$a_3 \wedge (a_2 \vee a_4) = a_3 \wedge a_1 = a_3,$$

但

$$(a_3 \wedge a_2) \vee (a_3 \wedge a_4) = a_5 \vee a_4 = a_4.$$



(a) 图 7-4 (b)

图 7-4(b) 中

$$b \wedge (c \vee d) = b \wedge a = b,$$

但 $(b \wedge c) \vee (b \wedge d) = e \vee e = e$. 应该指出，在分配格的定义中有些条件是多余的.

定理 7-11 在格 $\langle L; \vee, \wedge \rangle$ 中，如果交运算对并运算是可分配的，则并运算对交运算也是可分配的；如果并运算对交运算是可分配的，则交运算对并运算也是可分配的.

证明 设在格 $\langle L; \vee, \wedge \rangle$ 中，对任意的 $l_1, l_2, l_3 \in L$，

有 $$l_1 \wedge (l_2 \vee l_3) = (l_1 \wedge l_2) \vee (l_1 \wedge l_3),$$

则 $$\begin{aligned}(l_1 \vee l_2) \wedge (l_1 \vee l_3) &= [(l_1 \vee l_2) \wedge l_1] \vee [(l_1 \vee l_2) \wedge l_3] \\ &= l_1 \vee [(l_1 \vee l_2) \wedge l_3] = l_1 \vee [(l_1 \wedge l_3) \vee (l_2 \wedge l_3)] \\ &= [l_1 \vee (l_1 \wedge l_3)] \vee (l_2 \wedge l_3) = l_1 \vee (l_2 \wedge l_3).\end{aligned}$$

由对偶原理，如果并运算对交运算是可分配的，则交运算对并运算也是可分配的. 证完.

如果 $\langle L; \vee, \wedge \rangle$ 是分配格，则对任意的 $l, a_1, a_2, \cdots, a_n \in L$，有

$$l \vee \left(\bigwedge_{i=1}^{n} a_i\right) = \bigwedge_{i=1}^{n} (l \vee a_i),$$

$$l \wedge \left(\bigvee_{i=1}^{n} a_i\right) = \bigvee_{i=1}^{n} (l \wedge a_i).$$

更一般地，对于任意的 $l_1, l_2, \cdots, l_m, a_1, a_2, a_3, \cdots, a_n \in L$，有

$$\left(\bigwedge_{i=1}^{m} l_i\right) \vee \left(\bigwedge_{j=1}^{n} a_j\right) = \bigwedge_{i=1}^{m} \left(\bigwedge_{j=1}^{n} (l_i \vee a_j)\right),$$

$$\left(\bigvee_{i=1}^{m} l_i\right) \wedge \left(\bigvee_{j=1}^{n} a_j\right) = \bigvee_{i=1}^{m} \left(\bigvee_{j=1}^{n} (l_i \wedge a_j)\right).$$

定理 7-12 设 l_1, l_2, l_3 是分配格 $\langle L; \vee, \wedge \rangle$ 中的任意三个元素，则

$$(l_1 \vee l_2 = l_1 \vee l_3,\ l_1 \wedge l_2 = l_1 \wedge l_3) \Leftrightarrow (l_2 = l_3).$$

证明 从右到左的推断是明显的. 为了证明从左到右的推断，我们利用交换律、吸收律和分配律，

$$
\begin{aligned}
l_2 &= l_2 \vee (l_2 \wedge l_1) = l_2 \vee (l_3 \wedge l_1) \\
&= (l_2 \vee l_3) \wedge (l_2 \vee l_1) = (l_2 \vee l_3) \wedge (l_3 \vee l_1) \\
&= l_3 \vee (l_2 \wedge l_1) = l_3 \vee (l_3 \wedge l_1) \\
&= l_3\text{。证完。}
\end{aligned}
$$

如果一个格存在有最小元素和最大元素，则称它们为该格的**界**，并分别用 0 和 1 来表示。由最小元素和最大元素的定义，如果一个格 $(L;\vee,\wedge)$ 有元素 0 和 1，则对于所有的 $l \in L$，有 $l \leqslant 1$，$0 \leqslant l$。于是，由定理 7-3，对于所有的 $l \in L$，有

$$l \vee 1 = 1, \quad l \wedge 1 = l. \tag{7-10}$$

$$l \wedge 0 = 0, \quad l \vee 0 = l. \tag{7-11}$$

由 1 和 0 的唯一性可知，含有元素 1 和 0 的格的次序图中，必有唯一个称为"1"的结点，它位于图的最上层。有唯一个称为"0"的结点，它位于图的最下层。并且从任一其它结点出发经过向上的路径都可以到达结点 1，而从任一其它结点出发经过向下的路径都可以到达结点 0。

例如，在图 7-1 所给出的格 $(2^U; \cup, \cap)$ 的次序图中，结点 $\{a, b, c\}$ 代表元素 1，ϕ 代表元素 0。

又如，$(R; \leqslant)$（其中 R 是实数集，$\leqslant$ 是通常的"小于或等于"关系）显然是一个格。对于任意的 $r_1, r_2 \in R$，

$$\mathrm{glb}(r_1, r_2) = \min(r_1, r_2),$$

$$\mathrm{lub}(r_1, r_2) = \max(r_1, r_2).$$

但这个格既没有最大元素也没有最小元素。

定义 7-7 设 $(L;\vee,\wedge)$ 是一个含有元素 1 和 0 的格，对于 L 中的一个元素 l，若有元素 $\bar{l}$ 使得 $l \vee \bar{l} = 1$，$l \wedge \bar{l} = 0$，则称元素 $\bar{l}$ 是 l 的补。

显然，l 和 $\bar{l}$ 是互补的。即若 $\bar{l}$ 是 l 的一个补，则 l 也是 $\bar{l}$ 的一个补。

例如图 7-5 中的格，d 是 e 的一个补，同时 e 也是 d 的一个

补。一个元素可以有多于一个的补。例如图 7-5 中，b 和 e 都是 d 的补。但是另一方面，c 没有补。

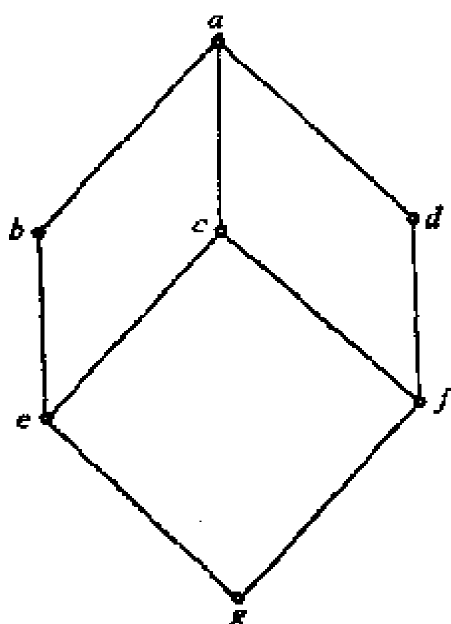


图 7-5

由 (7-10) 和 (7-11) 可知，0 和 1 互补。

定义 7-8 设 $\langle L;\vee,\wedge\rangle$ 是一个含有元素 1 和 0 的格，如果 L 中每一个元素都有补，则称 $\langle L;\vee,\wedge\rangle$ 为**有补格**。

例如，在图7-4 (a) 所给出的格中，每一个元素都有补。a_2 的补元是 a_3 和 a_4，a_3 和 a_4 的补元都是 a_2，a_1 和 a_5 互为补元。因此这是一个有补格。又如图7-4 (b) 所给出的格中，b 的补元是 c 和 d，c 的补元是 b 和 d，d 的补元是 b 和 c，a 和 e 互为补元。因此，它也是一个有补格。

又如，格 $\langle 2^U;\cup,\cap\rangle$ 是一个有补格。其中全集合 U 是元素1，空集 ϕ 是元素 0。U 的每一子集 S_i 的补元素是 S_i' (即 S_i 的补集)。

如果一个格既是有补格又是分配格，则称它为**有补分配格**。例如，格 $\langle 2^U;\cup,\cap\rangle$ 就是一个有补分配格。

下面我们来看看有补分配格的一些性质。

定理 7-13 在有补分配格 $\langle L;\vee,\wedge\rangle$ 中，任一元素 $l\in L$ 的补元素 $\bar{l}$ 是唯一的。

证明 假设有两个元素 l_1 和 l_2，使得

$$l\vee l_1=1,\qquad l\wedge l_1=0;$$

$$l\vee l_2=1,\qquad l\wedge l_2=0.$$

则有

$$l\vee l_1=l\vee l_2,\quad l\wedge l_1=l\wedge l_2.$$

由定理 7-12 有 $l_1=l_2$。因此 l 的补元素唯一。证完。

定理 7-14 (对合律)

在有补分配格⟨L; $\vee$, $\wedge$⟩中，对于任一元素 $l\in L$，有 $\bar{\bar{l}}=l$.

证明 因为 $l\vee\bar{l}=1, l\wedge\bar{l}=0$，由交换律有 $\bar{l}\vee l=1, \bar{l}\wedge l=0$。所以 l 是 $\bar{l}$ 的补. 又由定理 7-13, $\bar{l}$ 的补是唯一的, 故得 $\bar{\bar{l}}=l$. 证完。

定理 7-15 （德·摩根定律）

在有补分配格⟨L; $\vee$, $\wedge$⟩中，对于任意的 $l_1, l_2\in L$，有

$$(a)\ \overline{l_1\vee l_2}=\bar{l}_1\wedge\bar{l}_2,\quad (b)\ \overline{l_1\wedge l_2}=\bar{l}_1\vee\bar{l}_2.$$

证明 (a) 由分配律可知：

$$(l_1\vee l_2)\vee(\bar{l}_1\wedge\bar{l}_2)=(l_1\vee l_2\vee\bar{l}_1)\wedge(l_1\vee l_2\vee\bar{l}_2)=1\wedge1=1,$$

$$(l_1\vee l_2)\wedge(\bar{l}_1\wedge\bar{l}_2)=(l_1\wedge\bar{l}_1\wedge\bar{l}_2)\vee(l_2\wedge\bar{l}_1\wedge\bar{l}_2)=0\vee0=0.$$

由补的唯一性便有 $\overline{l_1\vee l_2}=\bar{l}_1\wedge\bar{l}_2$。

(b) 可由对偶原理推出。证完。

定理 7-16 在有补分配格⟨L; $\vee$, $\wedge$⟩中，对于任意的 l_1, $l_2\in L$，有

$$(l_1\leqslant l_2)\Leftrightarrow(l_1\wedge\bar{l}_2=0)\Leftrightarrow(\bar{l}_1\vee l_2=1)$$

证明 由定理 7-3 有

$$(l_1\leqslant l_2)\Leftrightarrow(l_1\vee l_2=l_2)\Leftrightarrow(l_1\wedge l_2=l_1),$$

又由德·摩根定律有

$$(l_1\leqslant l_2)\Leftrightarrow(\bar{l}_1\wedge\bar{l}_2=\bar{l}_2)\Leftrightarrow(\bar{l}_1\vee\bar{l}_2=\bar{l}_1),$$

因此，若 $l_1\leqslant l_2$，则

$$l_1\wedge\bar{l}_2=l_1\wedge(\bar{l}_1\wedge\bar{l}_2)=0,$$

且
$$\bar{l}_1\vee l_2=(\bar{l}_1\vee\bar{l}_2)\vee l_2=1.$$

反之，若 $l_1\wedge\bar{l}_2=0$，则

$$l_2=l_2\vee(l_1\wedge\bar{l}_2)=(l_2\vee l_1)\wedge(l_2\vee\bar{l}_2)=l_2\vee l_1,$$

因而有
$$l_1\leqslant l_2.$$

若 $\bar{l}_1\vee l_2=1$，则

$$l_1=l_1\wedge(\bar{l}_1\vee l_2)=(l_1\wedge\bar{l}_1)\vee(l_1\wedge l_2)=l_1\wedge l_2,$$

因而有
$$l_1\leqslant l_2$$

由上可知，

$$(l_1 \leqslant l_2) \Leftrightarrow (l_1 \wedge \bar{l}_2 = 0) \Leftrightarrow (\bar{l}_1 \vee l_2 = 1)\text{。证完。}$$

§7.5 布尔代数

定义 7-9 如果一个格既是分配格又是有补格，则称其为一个**布尔代数**。

因为在有补分配格中，每一元素的补都是唯一的，因此求补运算能够作为这种格的域上的一元运算。于是，具有域 B 的布尔代数可表示为 $\langle B; -, \vee, \wedge\rangle$（这里 $\vee$ 和 $\wedge$ 是原有的并与交运算，$-$ 是求补运算）。

由前面的讨论可知，一个布尔代数 $\langle B; -, \vee, \wedge\rangle$ 具有下列的基本性质：

对于 B 中的任意元素 x，y，z，有：

（1）**交换律** $x \vee y = y \vee x$，$x \wedge y = y \wedge x$；

（2）**结合律** $x \vee (y \vee z) = (x \vee y) \vee z$，

$x \wedge (y \wedge z) = (x \wedge y) \wedge z$；

（3）**等幂律** $x \vee x = x$，$x \wedge x = x$；

（4）**吸收律** $x \vee (x \wedge y) = x$，$x \wedge (x \vee y) = x$；

（5）**分配律** $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$，

$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$；

（6）**同一律** $x \vee 0 = x$，$x \wedge 1 = x$；

（7）**零一律** $x \vee 1 = 1$，$x \wedge 0 = 0$；

（8）**互补律** $x \vee \bar{x} = 1$，$x \wedge \bar{x} = 0$；

（9）**对合律** $\bar{\bar{x}} = x$；

（10）**德·摩根定律** $\overline{x \vee y} = \bar{x} \wedge \bar{y}$，$\overline{x \wedge y} = \bar{x} \vee \bar{y}$。

以上这十条性质并不都是独立的。事实上，所有其它的性质都可由其中的四条：交换律、分配律、同一律和互补律推导出来。

首先我们注意到，交换律、分配律、同一律和互补律这四条基本定律，每一条都包含了互为对偶的两个关系式。也就是说，如果在每一条基本定律中，将第一个关系式中的∨、∧、0、1分别改为∧、∨、1、0，则第一个关系式就变成了第二个关系式。因此与格一样，布尔代数的任一由这些基本关系式所导出的关系式的对偶，亦可由这些基本关系式的对偶导出。上述布尔代数的性质(2)、(3)、(4)、(7)、(10)中，每一条性质都包含了两个互为对偶的关系式，根据对偶原理，我们只要证明其中之一即可。

首先我们证明0和1二者都是唯一的。为此，我们假设有两个元素0和a对所有的$x\in B$都满足(6)中的第一个关系式，则根据交换律，有

$$a=a\vee 0=0\vee a=0。$$

同样地，若元素1和b对所有的$x\in B$都满足(6)中的第二个关系式，则又有

$$b=b\wedge 1=1\wedge b=1。$$

因此0和1都是唯一的。

下面我们证明互补律和"－"是B上的运算两者是一致的。

定理 7-17 对每一个$x\in B$，若有$y\in B$使得$x\vee y=1$，$x\wedge y=0$，则$y=\bar{x}$。

证明 $y=y\wedge 1$ (同一律)

$=y\wedge(x\vee\bar{x})$ (互补律)

$=(y\wedge x)\vee(y\wedge\bar{x})$ (分配律)

$=0\vee(y\wedge\bar{x})$ (交换律、假设)

$=(x\wedge\bar{x})\vee(y\wedge\bar{x})$ (互补律)

$=(\bar{x}\wedge x)\vee(\bar{x}\wedge y)$ (交换律)

$=\bar{x}\wedge(x\vee y)$ (分配律)

$=\bar{x}\wedge 1$ (假设)

$=\bar{x}$。 (同一律) 证完。

定理 7-18 （对合律）

对每一个 $x \in B$，$\bar{\bar{x}} = x$。

证明 由互补律，$x \vee \bar{x} = 1, x \wedge \bar{x} = 0$。又由交换律，$\bar{x} \vee x = 1$，$\bar{x} \wedge x = 0$。于是由定理7-17，$\bar{\bar{x}} = x$。证完。

定理 7-19 （等幂律）

对任意的 $x \in B$，有

$$(a)\ x \vee x = x, \quad (b)\ x \wedge x = x.$$

证明 (a) $x \vee x = (x \vee x) \wedge 1$ （同一律）

$= (x \vee x) \wedge (x \vee \bar{x})$ （互补律）

$= x \vee (x \wedge \bar{x})$ （分配律）

$= x \vee 0$ （互补律）

$= x$。 （同一律）证完。

定理 7-20 （零一律）

对任意的 $x \in B$，有

$$(a)\ x \vee 1 = 1, \quad (b)\ x \wedge 0 = 0.$$

证明 (a) $x \vee 1 = (x \vee 1) \wedge 1$ （同一律）

$= (x \vee 1) \wedge (x \vee \bar{x})$ （互补律）

$= x \vee (1 \wedge \bar{x})$ （分配律）

$= x \vee \bar{x}$ （交换律，同一律）

$= 1$。 （互补律）证完。

定理 7-21 （吸收律）

对任意的 $x, y \in B$，有

$$(a)\ x \vee (x \wedge y) = x, \quad (b)\ x \wedge (x \vee y) = x.$$

证明 (a) $x \vee (x \wedge y)$

$= (x \wedge 1) \vee (x \wedge y)$ （同一律）

$= x \wedge (1 \vee y)$ （分配律）

$= x \wedge 1$ （交换律、定理7-20）

$= x$。 （同一律）证完。

引理 对任意的 $x,y,z\in B$，若 $x\wedge y=x\wedge z$，$\bar{x}\wedge y=\bar{x}\wedge z$，则 $y=z$。

证明 因为

$$(x\wedge y)\vee(\bar{x}\wedge y)=y\wedge(x\vee\bar{x})=y\wedge 1=y,$$

$$(x\wedge z)\vee(\bar{x}\wedge z)=z\wedge(x\vee\bar{x})=z\wedge 1=z,$$

所以 $y=z$，证完。

定理 7-22 （结合律）

对任意的 $x,y,z\in B$，有

(a) $x\vee(y\vee z)=(x\vee y)\vee z$，(b) $x\wedge(y\wedge z)=(x\wedge y)\wedge z$。

证明 (a) 令 $L=x\vee(y\vee z)$，$M=(x\vee y)\vee z$，

则 $x\wedge L=x\wedge[x\vee(y\vee z)]=x$

且 $x\wedge M=x\wedge[(x\vee y)\vee z]=[x\wedge(x\vee y)]\vee(x\wedge z)$
$=x\vee(x\wedge z)=x$，

因此 $x\wedge L=x\wedge M$。

又因 $\bar{x}\wedge L=\bar{x}\wedge[x\vee(y\vee z)]=(\bar{x}\wedge x)\vee[\bar{x}\wedge(y\vee z)]$
$=0\vee[\bar{x}\wedge(y\vee z)]=(\bar{x}\wedge y)\vee(\bar{x}\wedge z)$，

而且 $\bar{x}\wedge M=\bar{x}\wedge[(x\vee y)\vee z]=[\bar{x}\wedge(x\vee y)]\vee(\bar{x}\wedge z)$
$=[(\bar{x}\wedge x)\vee(\bar{x}\wedge y)]\vee(\bar{x}\wedge z)=(\bar{x}\wedge y)\vee(\bar{x}\wedge z)$，

因此 $\bar{x}\wedge L=\bar{x}\wedge M$。

于是由引理，我们有 $L=M$；这就证明了并的结合律。

定理 7-23 （德·摩根定律）

对任意的 $x,y\in B$，有

(a) $\overline{x\vee y}=\bar{x}\wedge\bar{y}$，(b) $\overline{x\wedge y}=\bar{x}\vee\bar{y}$。

证明方法与定理 7-15 相同。

以上说明，与格一样布尔代数 $(B;-,\vee,\wedge)$ 也是一个代数系统，该代数系统可取交换律、分配律、同一律和互补律作为公理。显然，集合代数 $(2^U;',\cup,\cap)$ 是一个布尔代数。因为它满足布

尔代数的四条公理。因此，对于布尔代数 $\langle B; -, \vee, \wedge\rangle$ 推导出来的所有结论，对于集合代数都是成立的。

下面两个定理阐述了一个有趣的现象，即布尔代数的子代数以及布尔代数的满同态象仍是布尔代数。

定理 7-24 布尔代数的每一子代数仍是布尔代数。

证明 设 $\langle \tilde{B}; -, \vee, \wedge\rangle$ 是布尔代数 $\langle B; -, \vee, \wedge\rangle$ 的子代数。由子代数的定义可知，交换律和分配律在 $\langle \tilde{B}; -, \vee, \wedge\rangle$ 中仍然成立。又若 $x \in \tilde{B}$，则由封闭性有 $\bar{x} \in \tilde{B}$，因此 $x \vee \bar{x} = 1 \in \tilde{B}$，$x \wedge \bar{x} = 0 \in \tilde{B}$，所以互补律和同一律也成立。故定理得证。

定理 7-25 一个布尔代数的每一满同态象都是布尔代数。

证明 设 $\langle B_0; ', \cup, \cap\rangle$ 是布尔代数 $\langle B; -, \vee, \wedge\rangle$ 在满同态 h 下的同态象。由定理4-5知交换律和分配律在 $\langle B_0; ', \cup, \cap\rangle$ 中仍然成立。由布尔代数 $\langle B; -, \vee, \wedge\rangle$ 满足同一律，知 $h(1)$ 和 $h(0)$ 分别是 $\langle B_0; ', \cup, \cap\rangle$ 的 1 元素和 0 元素。即 $\langle B_0; ', \cup, \cap\rangle$ 满足同一律。又因为 h 是从 B 到 B_0 的满射，因此 B_0 中任一元素 x_0 都可表为 $h(x)$ 的形式，这里 $x \in B$。因此对于任一 $x_0 \in B_0$，有

$$h(0) = h(x \wedge \bar{x}) = h(x) \cap h(\bar{x}) = h(x) \cap (h(x))' = x_0 \cap x_0',$$

$$h(1) = h(x \vee \bar{x}) = h(x) \cup h(\bar{x}) = h(x) \cup (h(x))' = x_0 \cup x_0'.$$

即 $\langle B_0; ', \cup, \cap\rangle$ 满足互补律。

由上可知，$\langle B_0; ', \cup, \cap\rangle$ 是一个布尔代数。证完。

例 1 设 $U = \{u_1, u_2, u_3\}$。布尔代数 $\langle 2^U; ', \cap, \cup\rangle$ 有子代数：

$$\langle\{\Phi, U\}; ', \cup, \cap\rangle,$$

$$\langle\{\Phi, \{u_1\}, \{u_2, u_3\}, U\}; ', \cup, \cap\rangle,$$

$$\langle\{\Phi, \{u_2\}, \{u_1, u_3\}, U\}; ', \cup, \cap\rangle,$$

$$\langle\{\Phi, \{u_3\}, \{u_1, u_2\}, U\}; ', \cup, \cap\rangle.$$

它们都是尔布代数。

表7-1和表7-2定义了这些代数的运算(为了方便起见，后三个代数的域都用 $\{\Phi, S, T, U\}$ 表示)。

表7-1 $\langle\{\Phi, U\};\ ', \cup, \cap\rangle$ 的运算表

x	$\bar{x}$
Φ	U
U	Φ

$\cup$	Φ	U
Φ	Φ	U
U	U	U

$\cap$	Φ	U
Φ	Φ	Φ
U	Φ	U

表7-2 $\langle\{\Phi, S, T, U\};\ ', \cup, \cap\rangle$ 的运算表

x	$\bar{x}$
Φ	U
S	T
T	S
U	Φ

$\cup$	Φ	S	T	U
Φ	Φ	S	T	U
S	S	S	U	U
T	T	U	T	U
U	U	U	U	U

$\cap$	Φ	S	T	U
Φ	Φ	Φ	Φ	Φ
S	Φ	S	Φ	S
T	Φ	Φ	T	T
U	Φ	S	T	U

例 2 设 $U=\{u_1, u_2, u_3\}$。定义集合 2^U 上的关系 ρ：当且仅当 $\{u_1\}\cap S=\{u_1\}\cap T$ 时，有 $S\rho T$。显然，这是一个等价关系。而且如果 $\{u_1\}\cap S=\{u_1\}\cap T$，则有 $\{u_1\}\cap S'=\{u_1\}\cap T'$，

即由 $S\rho T$ 可得 $S'\rho T'$。

又如果 $\{u_1\}\cap S_1=\{u_1\}\cap T_1$ 且 $\{u_1\}\cap S_2=\{u_1\}\cap T_2$，

则有 $$\{u_1\}\cap(S_1\cup S_2)=\{u_1\}\cap(T_1\cup T_2)$$

且 $$\{u_1\}\cap(S_1\cap S_2)=\{u_1\}\cap(T_1\cap T_2),$$

即由 $$S_1\rho T_1,\ S_2\rho T_2,$$

可得 $$(S_1\cup S_2)\rho(T_1\cup T_2),\ (S_1\cap S_2)\rho(T_1\cap T_2).$$

于是，ρ 是布尔代数 $\langle 2^U;\ ', \cup, \cap\rangle$ 上的同余关系. 这一同余关系可导致 2^U 上一等价分划

$$\pi_\rho^{2^n}=\{\{\Phi, \{u_2\}, \{u_3\}, \{u_2, u_3\}\}, \{U, \{u_1\}, \{u_1, u_2\}, \{u_1, u_3\}\}\}$$
$$=\{[\Phi]_\rho, [U]_\rho\}.$$

由定理 4-9，相应存在一个由函数 $h: 2^U\to\{[\phi]_\rho, [U]_\rho\}$ 给出的从 $\langle 2^U;\ ', \cup, \cap\rangle$ 到 $\langle\{[\Phi]_\rho, [U]_\rho\};\ ', \cup, \cap\rangle$ 的满同态. 这里对于每一 $S\in 2^U$, $h(S)=[S]_\rho$, $\langle\{[\phi]_\rho, [U]_\rho\};\ ', \cup, \cap\rangle$ 的运算规定为(在

表 7-3 中给出)

$$([S]_\rho)' = [S']_\rho,$$
$$[S_1]_\rho \cup [S_2]_\rho = [S_1 \cup S_2]_\rho,$$
$$[S_1]_\rho \cap [S_2]_\rho = [S_1 \cap S_2]_\rho.$$

因为 $\langle 2^U; ', \cup, \cap \rangle$ 是布尔代数，由定理 7-25，$\langle \{[\phi]_\rho, [U]_\rho\}; ', \cup, \cap \rangle$ 也是一布尔代数 这一事实也可由比较表 7-1 和表 7-3，$\langle \{[\phi]_\rho, [U]_\rho\}; ', \cup, \cap \rangle$ 与 $\langle \{\phi, U\}; ', \cup, \cap \rangle$ 是同构的而得到证实。

表7-3 $\langle \{[\Phi]_\rho, [U]_\rho\}; ', \cup, \cap \rangle$ 的运算表

x	x'
$[\Phi]_\rho$	$[U]_\rho$
$[U]_\rho$	$[\Phi]_\rho$

$\cup$	$[\Phi]_\rho$	$[U]_\rho$
$[\Phi]_\rho$	$[\Phi]_\rho$	$[U]_\rho$
$[U]_\rho$	$[U]_\rho$	$[U]_\rho$

$\cap$	$[\Phi]_\rho$	$[U]_\rho$
$[\Phi]_\rho$	$[\Phi]_\rho$	$[\Phi]_\rho$
$[U]_\rho$	$[\Phi]_\rho$	$[U]_\rho$

§7·6 布尔代数的原子表示

定义 7-10 设 $\langle B; -, \vee, \wedge \rangle$ 是布尔代数，如果元素 $a \neq 0$，且对于每一个 $x \in B$，有 $x \wedge a = a$ 或 $x \wedge a = 0$，则称 a 是**原子**。

由原子的定义，若 a 是原子，则不存在任何元素 c，使得 $0 < c$，$c < a$。即原子 a 是仅比 0 元素"大"的元素。在 B 的次序图上，原子 a 是从结点 0 出发经过一条边就能到达的那些结点。

例 1 设 $U = \{u_1, u_2, u_3\}$，则布尔代数 $\langle 2^U; ', \cup, \cap \rangle$ 中，元素 $\{u_1\}, \{u_2\}, \{u_3\}$ 都是原子(图7-6)。

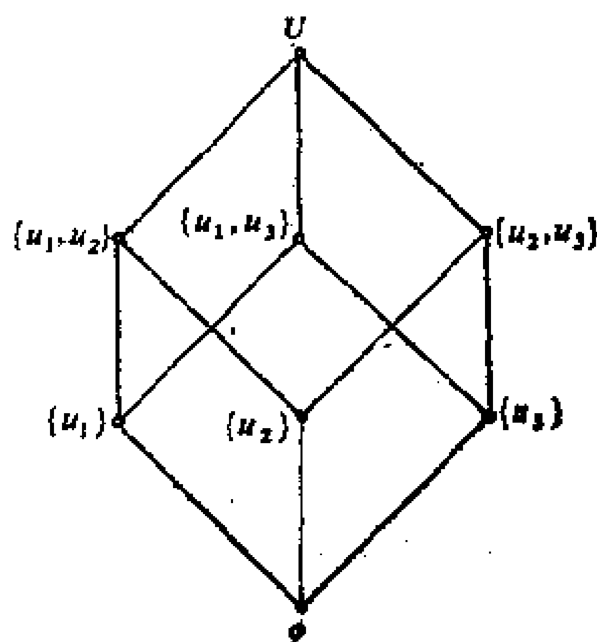


图 7-6

定理 7-26 设 $\langle B; -, \vee, \wedge\rangle$ 是一有限布尔代数，则对于每一非零的 $x \in B$，一定存在一个原子 a，使得 $x \wedge a = a$（或 $a \leqslant x$）。

证明 如果 x 是一个原子，则定理显然成立。如果 x 不是原子，则必存在某个元素 y，使得 $y \wedge x \neq x$ 且 $y \wedge x \neq 0$，令 $y \wedge x = x_1$，即有非零元素 $x_1 \neq x$，满足 $x_1 \leqslant x$。类似地，或者 x_1 是一个原子，或者存在一个非零元素 $x_2 \neq x_1$，满足 $x_2 \leqslant x_1$；或者 x_2 是一个原子，或者存在一个非零元素 $x_3 \neq x_2$，满足 $x_3 \leqslant x_2$，等等。因而得到一个序列

$$x \geqslant x_1 \geqslant x_2 \geqslant x_3 \geqslant \cdots,$$

由于 B 是有限的，故序列必终止于"小于或等于" x 的某个原子 a。证完。

定理 7-27 如果 a_1 和 a_2 是布尔代数 $\langle B; -, \vee, \wedge\rangle$ 的原子，且 $a_1 \wedge a_2 \neq 0$，则 $a_1 = a_2$。

证明 因为 $a_1 \wedge a_2 \neq 0$，所以由定义 7-10，有 $a_1 \wedge a_2 = a_1$ 且 $a_1 \wedge a_2 = a_2$，故有 $a_1 = a_2$。证完。

定理 7-28 设 $\langle B; -, \vee, \wedge\rangle$ 是一有限布尔代数，又 x 是 B 的任意一个非零元素，$a_1, a_2, \cdots, a_n$ 是 $\langle B; -, \vee, \wedge\rangle$ 中满足 $a_i \leqslant x$ 的所有原子，则

$$x = a_1 \vee a_2 \vee \cdots \vee a_n.$$

证明 设 $y = a_1 \vee a_2 \vee \cdots \vee a_n$，由（7-7′）有 $y \leqslant x$，则只须证 $x \leqslant y$。由定理 7-16 只须证 $x \wedge \bar{y} = 0$。现假设 $x \wedge \bar{y} \neq 0$，由定理 7-26 知必存在一原子 a，使得 $a \leqslant x \wedge \bar{y}$。而由（7-4）有 $x \wedge \bar{y} \leqslant x$ 且 $x \wedge \bar{y} \leqslant \bar{y}$，由传递性可得 $a \leqslant x$ 且 $a \leqslant \bar{y}$。同时因为 $a \leqslant x$，则存在某一 a_i（$1 \leqslant i \leqslant n$），使得 $a = a_i$。由（7-6′）有 $a \leqslant a_1 \vee a_2 \vee \cdots \vee a_n = y$，于是我们有 $a \leqslant y$ 且 $a \leqslant \bar{y}$。由（7-5）可知，$a \leqslant y \wedge \bar{y} = 0$，即得到 $a = 0$。这与 a 是原子相矛盾。因此必须有 $x \wedge \bar{y} = 0$，即 $x \leqslant y$。最后由反对称性，得 $x = a_1 \vee a_2 \vee \cdots \vee a_n$。证完。

定理 7-29 设 $\langle B; -, \vee, \wedge\rangle$ 是一有限布尔代数，x 是 B 的任意一个非零元素，$a_1, a_2, \cdots, a_n$ 是 $\langle B; -, \wedge, \wedge\rangle$ 中满足 $a_i \leqslant x$ 的所有原子，则 $x = a_1 \vee a_2 \vee \cdots \vee a_n$ 是将 x 表示为原子的并的唯一方式。

证明 设还有将 x 表示为原子的并的另一种表达式

$$x = b_1 \vee b_2 \vee \cdots \vee b_m.$$

显然，因为 x 是 $b_1, b_2, \cdots, b_m$ 的最小上界，所以有

$$b_1 \leqslant x,\ \ b_2 \leqslant x, \cdots, b_m \leqslant x,$$

这就意味着

$$\{b_1, b_2, \cdots, b_m\} \subseteq \{a_1, a_2, \cdots, a_n\}.$$

对于任一原子 a_i $(1 \leqslant i \leqslant n)$，因为 $a_i \leqslant x$，所以有 $a_i \wedge x = a_i$。因此

$$a_i \wedge (b_1 \vee b_2 \vee \cdots \vee b_m) = (a_i \wedge b_1) \vee (a_i \wedge b_2) \vee \cdots \vee (a_i \wedge b_m) = a_i,$$

于是，必有某一个 $b_j (1 \leqslant j \leqslant m)$，使得 $a_i \wedge b_j \neq 0$，由定理 7-27，有 $a_i = b_j$，即 $a_i \in \{b_1, b_2, \cdots, b_m\}$。因此有

$$\{a_1, a_2, \cdots, a_n\} \subseteq \{b_1, b_2, \cdots, b_m\}.$$

由上可得 $\{a_1, a_2, \cdots, a_n\} = \{b_1, b_2, \cdots, b_m\}$.

这就证明了 $x = a_1 \vee a_2 \vee \cdots \vee a_n$ 是将 x 表示为原子的并的唯一方式。证完。

定理 7-29 的结论使得在一个有限布尔代数 $\langle B; -, \vee, \wedge\rangle$ 的元素与它的所有原子的集合 M 的子集之间建立了一个一一对应关系。这种一一对应关系实际上是从 $\langle B; -, \vee, \wedge\rangle$ 到 $\langle 2^M; ', \cup, \cap\rangle$ 的一个同构。因此我们得到每一个有限的布尔代数必与某一集合代数同构的重要结果。

定理 7-30 设 $\langle B; -, \vee, \wedge\rangle$ 是一有限布尔代数，M 表示该代数所有原子的集合，则 $\langle B; -, \vee, \wedge\rangle$ 与 $\langle 2^M; ', \cup, \cap\rangle$ 同构。

证明 定义函数 $h: B\to 2^M$，

这里

$$h(x)=\begin{cases}\Phi & x=0;\\ \{a \mid a\in M, a\leqslant x\} & x\neq 0.\end{cases}$$

由定理 7-28 和定理 7-29 知 h 是一个双射。

对于任意非零元素 $x_1, x_2\in B$，设

$$h(x_1)=M_1=\{a_{11}, a_{12}, \cdots, a_{1k_1}\},$$
$$h(x_2)=M_2=\{a_{21}, a_{22}, \cdots, a_{2k_2}\},$$

因此 $\quad x_1=a_{11}\vee a_{12}\vee\cdots\vee a_{1k_1},\ x_2=a_{21}\vee a_{22}\vee\cdots\vee a_{2k_2}.$

$$x_1\vee x_2=a_{11}\vee a_{12}\vee\cdots\vee a_{1k_1}\vee a_{21}\vee a_{22}\vee\cdots\vee a_{2k_2}.$$

于是
$$h(x_1\vee x_2)=M_1\cup M_2. \tag{7-12}$$

其次，由分配律知

$$x_1\wedge x_2=(a_{11}\vee a_{12}\vee\cdots\vee a_{1k_1})\wedge(a_{21}\vee a_{22}\vee\cdots\vee a_{2k_2})$$
$$=\bigvee_{i=1}^{k_1}\left(\bigvee_{j=1}^{k_2}(a_{1i}\wedge a_{2j})\right),$$

由定理 7-27

$$a_{1i}\wedge a_{2j}=\begin{cases}a_{1i}=a_{2j} & \text{若 } a_{1i}=a_{2j};\\ 0 & a_{1i}\neq a_{2j}.\end{cases}$$

因此，$x_1\wedge x_2$ 等于所有使得 $a_{1i}=a_{2j}$ 的 a_{1i}（或 a_{2j}）的并。结果可得

$$h(x_1\wedge x_2)=M_1\cap M_2. \tag{7-13}$$

最后，假设 $x_2=\bar{x}_1$，则

$x_1\vee x_2=1$，因此 $h(x_1\vee x_2)=M_1\cup M_2=M.$

又 $\quad x_1\wedge x_2=0$，因此 $h(x_1\wedge x_2)=M_1\cap M_2=\phi.$

结果有
$$M_2=M_1'.\ \text{即 } h(\bar{x}_1)=(h(x_1))'. \tag{7-14}$$

当 x_1 和 x_2 是非零的假设去掉。即当 $x_1=0$ 或 $x_2=0$ 时，则 $M_1=\Phi$ 或 $M_2=\Phi$。(7-12)，(7-13) 和 (7-14) 立即可得。由此可知 h 是从 $\langle B; -, \vee, \wedge\rangle$ 到 $\langle 2^M; ', \cup, \cap\rangle$ 的同构。于是这两个

代数系统是同构的。证完。

定理7-30很重要，它说明我们可以用集合代数$\langle 2^M; ', \cup, \cap\rangle$来表示每一个有限布尔代数$\langle B; -, \vee, \wedge\rangle$。这个结论的一个直接推论是$\# B = 2^{\# M}$。由这个推论又可推出下面的结果：如果两个有限的布尔代数$\langle B_1; -, \vee, \wedge\rangle$和$\langle B_2; -, \vee, \wedge\rangle$的域有相同的基数，则它们的原子的集合也一定有相同的基数$\# M_1 = \# M_2$，于是，集合代数$\langle 2^{M_1}; ', \cup, \cap\rangle$与$\langle 2^{M_2}; ', \cup, \cap\rangle$同构，因而$\langle B_1; -, \vee, \wedge\rangle$与$\langle B_2; -, \vee, \wedge\rangle$同构。总之，我们有

定理7-31 每一有限布尔代数的域的基数都是2的幂，域具有相同基数的布尔代数必同构。

例2 设$A_1, A_2, \cdots, A_r$是全集合U的子集。如果S表示所有由$A_1, A_2, \cdots, A_r$产生的集合的集合，则$\langle S; ', \cup, \cap\rangle$是一个布尔代数（参看习题第17题）。对于$S$的每一个元素来说，由$A_1, A_2, \cdots, A_r$所产生的最小集或被包含于该元素中，或与该元素交为空集。因此，由$A_1, A_2, \cdots, A_r$产生的最小集是$\langle S; ', \cup, \cap\rangle$的原子。由定理7-30，$\langle S; ', \cup, \cap\rangle$与$\langle 2^M; ', \cup, \cap\rangle$同构。这里$M$是所有由$A_1, A_2, \cdots, A_r$所产生的最小集的集合。

例如，如果S是由X、Y产生的所有集合的集合，则布尔代数$\langle S; ', \cup, \cap\rangle$与$\langle 2^M; ', \cup, \cap\rangle$同构。这里$M = \{X\cap Y, X\cap Y', X'\cap Y, X'\cap Y'\}$（参见图7-7）。

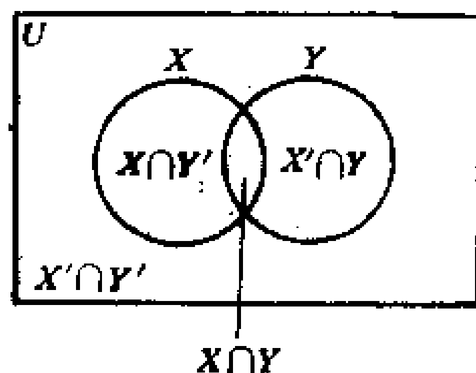


图7-7

$\langle 2^M;\ ',\ \cup,\ \cap\rangle$的次序图如图 7-8 所示。其中

$$A = X\cap Y,\ B = X\cap Y',\ C = X'\cap Y,\ D = X'\cap Y'.$$

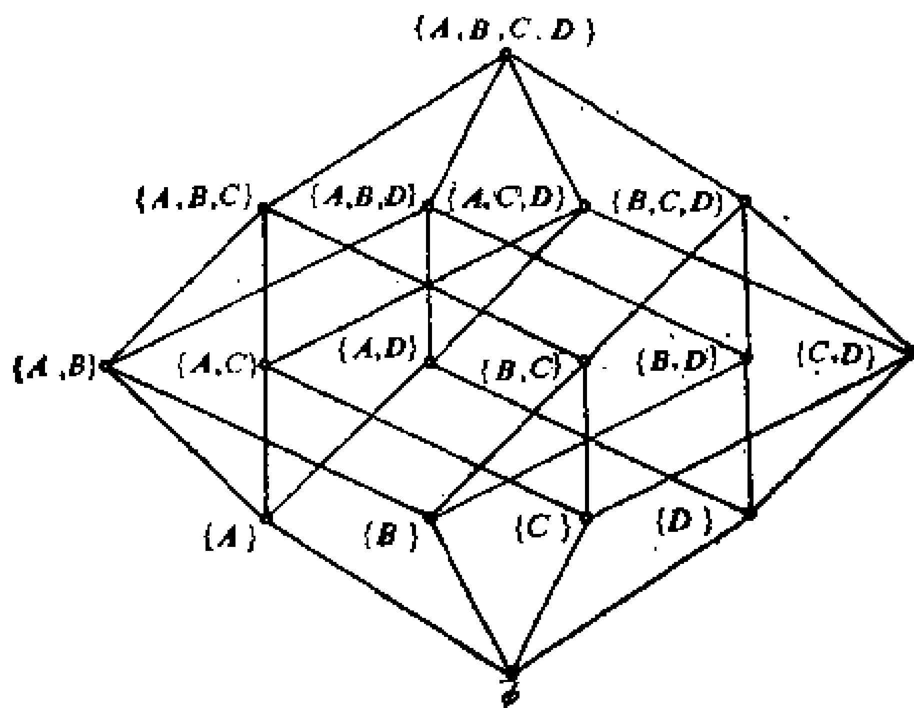


图 7-8

§7.7 布尔代数W_2^r

含有 n 个元素的布尔代数用 $W_n = \langle B_n;\ -,\ \vee,\ \wedge\rangle$ 表示。由定理 7-31 可知，n 必为 2 的幂，于是，"最小的"布尔代数就是 $W_2 = \langle B_2;\ -,\ \vee,\ \wedge\rangle$ [注]，其域 $B_2 = \{0, 1\}$。运用同一律、等幂律和零一律可得 W_2 的运算表如表 7-4。表 7-5 则定义了 $W_4 = \langle B_4;\ -,\ \vee,\ \wedge\rangle$的运算，这里 $B_4 = \{0, \alpha, \beta, 1\}$。(请比较表 7-1、表 7-2 与表7-4、表7-5)。

表7-4　W_2的运算表

x	$\bar{x}$
0	1
1	0

$\vee$	0	1
0	0	1
1	1	1

$\wedge$	0	1
0	0	0
1	0	1

[注] 不考虑只含有一个元素的布尔代数。

表7-5　W_4的运算表

x	$\bar{x}$
0	1
α	β
β	α
1	0

	0	α	β	1
0	0	α	β	1
α	α	α	1	1
β	β	1	β	1
1	1	1	1	1

$\wedge$	0	α	β	1
0	0	0	0	0
α	0	α	0	α
β	0	0	β	β
1	0	α	β	1

现在我们来考察 r 个布尔代数 W_2 的积代数 $W_2\times W_2\times\cdots\times W_2$（$r$ 次）。这个代数系统用 W_2^r 表示。它所用的运算符号与 W_2 相应的符号一样。即 $W_2^r=\langle B_2^r;-,\vee,\wedge\rangle$，其中

$$B_2^r=\underbrace{B_2\times B_2\times\cdots\times B_2}_{r\text{次}}=\{(x_1,x_2,\cdots,x_r)\mid x_i\in B_2,\ i=1,2,\cdots,r\}。$$

对于任意的 $(x_1,x_2,\cdots,x_r)$，$(y_1,y_2,\cdots,y_r)\in B_2^r$，有

$$\overline{(x_1,x_2,\cdots,x_r)}=(\bar{x}_1,\bar{x}_2,\cdots,\bar{x}_r),$$

$$(x_1,x_2,\cdots,x_r)\vee(y_1,y_2,\cdots,y_r)=(x_1\vee y_1,x_2\vee y_2,\cdots,x_r\vee y_r),$$

$$(x_1,x_2,\cdots,x_r)\wedge(y_1,y_2,\cdots,y_r)=(x_1\wedge y_1,x_2\wedge y_2,\cdots,x_r\wedge y_r)。$$

由定理4-11我们知道，W_2 的交换律、分配律和同一律均在 W_2^r 中保持有效（W_2^r 的零和一分别是 $(0,0,\cdots,0)$ 和 $(1,1,\cdots,1)$）。在 W_2^r 中有互补律成立也是容易证明的。因此，我们得到结论：W_2^r 是一个布尔代数，而且由定理7-31有

定理7-32　布尔代数 W_2^r 与 W_{2^r} 是同构的。任一有限布尔代数必与某一布尔代数 W_2^r 同构。

例1　表7-6给出了 $W_2^2=\langle B_2^2;-,\vee,\wedge\rangle$ 的运算，与表7-5比较可以证明，W_2^2 与 W_4 是同构的。

表7-6　W_2^2的运算表

x	$\bar{x}$
(0,0)	(1,1)
(0,1)	(1,0)
(1,0)	(0,1)
(1,1)	(0,0)

$\vee$	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	(0,1)	(1,0)	(1,1)
(0,1)	(0,1)	(0,1)	(1,1)	(1,1)
(1,0)	(1,0)	(1,1)	(1,0)	(1,1)
(1,1)	(1,1)	(1,1)	(1,1)	(1,1)

$\wedge$	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
(0,1)	(0,0)	(0,1)	(0,0)	(0,1)
(1,0)	(0,0)	(0,0)	(1,0)	(1,0)
(1,1)	(0,0)	(0,1)	(1,0)	(1,1)

在代数系统 $\langle 2^U; ', \cup, \cap\rangle$（这里 $U=\{u_1,u_2,\cdots,u_r\}$）和布尔代数 $W_2^r=\langle B_2^r; -, \cup, \cap\rangle$ 之间存在着一个同构关系。这个同构关系可由下式给出：

h：$2^U \to B_2^r$，这里

$h(S)=(x_1,x_2,\cdots,x_r)$，

$$x_i=\begin{cases}1 & \text{若 } u_i\in S\\ 0 & \text{否则}\end{cases} \quad (i=1,2,\cdots,r)$$

例如，当 $r=4$ 时，$h(\{u_1,u_3,u_4\})=(1,0,1,1)$。（参见§3.1例 11）。关于 h 是同构的证明，请读者自己作为练习给出。这一同构关系的存在证实了每一有限布尔代数都和某一集合代数同构的结论。

§7.8 布尔表达式和布尔函数

布尔代数 $\langle B; -, \vee, \wedge\rangle$ 上由 $x_1,x_2,\cdots,x_n$ 产生的**布尔表达式**可归纳地定义如下：

(1) B 的任意元素和任一符号 $x_1,x_2,\cdots,x_n$（不能与 B 的元素的名字相同）都是 $\langle B; -, \vee, \wedge\rangle$ 上由 $x_1,x_2,\cdots,x_n$ 产生的布尔表达式。

(2) 如果 e_1 和 e_2 是 $\langle B; -, \vee, \wedge\rangle$ 上由 $x_1,x_2,\cdots,x_n$ 产生的布尔表达式，则 (e_1)，$\bar{e}_1$，$(e_1\vee e_2)$，$(e_1\wedge e_2)$ 也是 $\langle B; -, \vee, \wedge\rangle$ 上由 $x_1,x_2,\cdots,x_n$ 产生的布尔表达式（括号在 $\wedge$ 优先于 $\vee$ 的约定下可省略）。

例如，$0\wedge\bar{1}$，$1\vee(\alpha\wedge x_1)\vee(\bar{x}_2\wedge x_3)$ 和 $\overline{(\beta\vee x_1\vee x_3)}\wedge 0$ 都是布尔代数 $\langle\{0,\alpha,\beta,1\}; -, \vee, \wedge\rangle$ 上由 x_1,x_2,x_3,x_4 产生的布尔表达式。

如果 $x_1,x_2,\cdots,x_n$ 被解释为只能从 B 中取值的变量，那么变量 $x_1,x_2,\cdots,x_n$ 的每一组取值对应着集合 B^n 上的一个有序 n 元

组，而$\langle B;-,\vee,\wedge\rangle$上由$x_1,x_2,\cdots,x_n$产生的布尔表达式可认为是表示$B$中的元素。于是，一个布尔表达式可以解释为形如$f:B^n\to B$的函数。这里，对于每一组特定的自变量$(x_1,x_2,\cdots,x_n)$，$f(x_1,x_2,\cdots,x_n)$能够由$\langle B;-,\vee,\wedge\rangle$上$-$、$\vee$、$\wedge$运算的定义所确定。因此，$\langle B;-,\vee,\wedge\rangle$上由$x_1,x_2,\cdots,x_n$产生的布尔表达式有时也被称为是$\langle B;-,\vee,\wedge\rangle$上$n$个变量的**布尔函数**。

例 1 下面是布尔代数$\langle\{0,\alpha,\beta,1\};-,\vee,\wedge\rangle$上由$x,y$产生的布尔表达式（或一个两变量的布尔函数）。

$$f(x,y)=(\beta\wedge\bar{x}\wedge y)\vee(\beta\wedge x\wedge(\overline{x\vee\bar{y}}))\vee(\alpha\wedge(x\vee(\bar{x}\wedge y))).$$

运用表 7-5 我们有，例如

$$f(\alpha,0)=(\beta\wedge\beta\wedge 0)\vee(\beta\wedge\alpha\wedge(\overline{\alpha\vee 1}))\vee(\alpha\wedge(\alpha\vee(\beta\wedge 0)))$$
$$=(\beta\wedge\alpha\wedge(\beta\wedge 0))\vee(\alpha\wedge\alpha)=\alpha.$$

表 7-7 列出了对于所有变量$(x,y)\in B^2$，$f(x,y)$的值。

表 7-7

x	y	$f(x,y)$
0	0	0
0	α	α
0	β	β
0	1	1
α	0	α
α	α	α
α	β	1
α	1	1
β	0	0
β	α	α
β	β	0
β	1	α
1	0	α
1	α	α
1	β	α
1	1	α

如果两个n变量的布尔表达式$f_1(x_1,x_2,\cdots,x_n)$和$f_2(x_1,x_2,\cdots,x_n)$，对于n个变量的任意一组赋值，都有相同的值，则称这两个布尔表达式是等价的。我们记作

$$f_1(x_1,x_2,\cdots,x_n)=f_2(x_1,x_2,\cdots,x_n).$$

例如，可以验证，布尔表达式$(x_1\wedge x_2)\vee(x_1\wedge\bar{x}_3)$和$x_1\wedge(x_2\vee\bar{x}_3)$是等价的。因此，我们推导一个布尔表达式或化简一个布尔表达式，它的意思就是将其推导或化简为一个等价形式。因为在布尔表达式中变量所取的值是B中的元素，所以前几节所导出的关于布尔代数的所有恒等式都可以用来处理和化简布尔表达式。

例如 $$\begin{aligned} x_1 \wedge x_2 &= (x_1 \wedge x_2) \wedge 1 \\ &= (x_1 \wedge x_2) \wedge (x_3 \vee \bar{x}_3) \\ &= (x_1 \wedge x_2 \wedge x_3) \vee (x_1 \wedge x_2 \wedge \bar{x}_3). \end{aligned}$$

定义 7-11 布尔代数 $\langle B; -, \vee, \wedge \rangle$ 上由 $x_1, x_2, \cdots, x_n$ 产生的形如 $\hat{x}_1 \wedge \hat{x}_2 \wedge \cdots \wedge \hat{x}_n$ 的布尔表达式称为由 $x_1, x_2, \cdots, x_n$ 产生的**最小项**，其中 $\hat{x}_i$ 或为 x_i 或为 $\bar{x}_i$。

例如，$x_1 \wedge x_2 \wedge x_3 \wedge x_4$，$\bar{x}_1 \wedge x_2 \wedge \bar{x}_3 \wedge x_4$，$x_1 \wedge \bar{x}_2 \wedge x_3 \wedge x_4$ 均是由 x_1, x_2, x_3, x_4 产生的最小项。

通常用记号 $m_{\delta_1\delta_2\cdots\delta_n}$ 来表示最小项，
其中

$$\delta_i = \begin{cases} 1 & \text{当 } \hat{x}_i = x_i; \\ 0 & \text{当 } \hat{x}_i = \bar{x}_i. \end{cases}$$

例如，上述三个由 x_1, x_2, x_3, x_4 产生的最小项可分别表示为：

$$m_{1111}, \quad m_{0101}, \quad m_{1011}.$$

定义 7-12 布尔代数 $\langle B; -, \vee, \wedge \rangle$ 上由 $x_1, x_2, \cdots, x_n$ 产生的形如 $\hat{x}_1 \vee \hat{x}_2 \vee \cdots \vee \hat{x}_n$ 的布尔表达式称为由 $x_1, x_2, \cdots, x_n$ 产生的**最大项**，其中 $\hat{x}_i$ 或为 x_i 或为 $\bar{x}_i$。

例如，$x_1 \vee x_2 \vee x_3 \vee x_4$，$\bar{x}_1 \vee x_2 \vee \bar{x}_3 \vee x_4$，$x_1 \vee \bar{x}_2 \vee x_3 \vee x_4$ 均是由 x_1, x_2, x_3, x_4 产生的最大项。

通常用记号 $\tilde{m}_{\delta_1\delta_2\cdots\delta_n}$ 来表示最大项，
其中

$$\delta_i = \begin{cases} 0 & \text{当 } \hat{x}_i = x_i; \\ 1 & \text{当 } \hat{x}_i = \bar{x}_i. \end{cases}$$

例如，上述三个最大项可分别表示为：$\tilde{m}_{0000}, \tilde{m}_{1010}, \tilde{m}_{0100}$。

定理 7-33 布尔代数 $\langle B; -, \vee, \wedge \rangle$ 上由 $x_1, x_2, \cdots, x_n$ 产生的每一布尔表达式均能表示成如下形式：

$$f(x_1, x_2, \cdots, x_n) = \bigvee_{k=00\cdots0}^{11\cdots1} (c_k \wedge m_k). \tag{7-15}$$

$$f(x_1, x_2, \cdots, x_n) = \bigwedge_{k=00\cdots0}^{11\cdots1} (c_k \vee \tilde{m}_k). \tag{7-16}$$

这里k取所有2^n个可能的值$\delta_1\delta_2\cdots\delta_n(\delta_i\in\{0,1\})$，由$c_k=c_{\delta_1\delta_2\cdots\delta_n}=f(\delta_1,\delta_2,\cdots,\delta_n)$。

例如，假设$f(x_1,x_2,x_3)$是$\langle B;-,\vee,\wedge\rangle$上由$x_1,x_2,x_3$产生的一个布尔表达式，根据(7-15)式，它可以表示成如下形式：

$$
\begin{aligned}
f(x_1,x_2,x_3)&=[c_{000}\wedge m_{000}]\vee[c_{001}\wedge m_{001}]\vee\cdots\vee[c_{110}\wedge m_{110}]\\
&\quad\vee[c_{111}\wedge m_{111}]\\
&=[f(0,0,0)\wedge\bar{x}_1\wedge\bar{x}_2\wedge\bar{x}_3]\vee[f(0,0,1)\wedge\bar{x}_1\wedge\bar{x}_2\wedge x_3]\vee\\
&\quad\cdots\vee[f(1,1,0)\wedge x_1\wedge x_2\wedge\bar{x}_3]\vee[f(1,1,1)\wedge x_1\wedge x_2\wedge x_3]。
\end{aligned}
$$

下面给出(7-15)式的证明。(7-16)式的证明完全类似。

证明 (对变量的个数进行归纳)

对于单变量布尔函数$f(x)$，(7-15)式是成立的。

首先，如果$f(x)=x$，则

$$x=(0\wedge\bar{x})\vee(1\wedge x)=(f(0)\wedge\bar{x})\vee(f(1)\wedge x)。$$

即
$$f(x)=(f(0)\wedge\bar{x})\vee(f(1)\wedge x)。$$

如果$f(x)=k$（不含x的式子），则$f(0)=f(1)=k$。

因而
$$f(x)=(k\wedge\bar{x})\vee(k\wedge x)=(f(0)\wedge\bar{x})\vee(f(1)\wedge x)。$$

其次，如果(7-15)式对某一函数$f(x)$成立，则对其补$\overline{f(x)}$也成立．因为

$$
\begin{aligned}
\overline{f(x)}&=\overline{((f(0)\wedge\bar{x})\vee(f(1)\wedge x))}\\
&=(\overline{f(0)}\vee x)\wedge(\overline{f(1)}\vee\bar{x})\\
&=(\overline{f(0)}\wedge\bar{x})\vee(\overline{f(1)}\wedge x)。
\end{aligned}
$$

此外，如果(7-15)式对函数$f(x)$，$g(x)$都成立，则对它们的并和交也成立。这是因为

$$
\begin{aligned}
f(x)\vee g(x)&=[(f(0)\wedge\bar{x})\vee(f(1)\wedge x)]\vee[(g(0)\wedge\bar{x})\vee(g(1)\wedge x)]\\
&=[(f(0)\vee g(0))\wedge\bar{x}]\vee[(f(1)\vee g(1))\wedge x],
\end{aligned}
$$

$$
\begin{aligned}
f(x)\wedge g(x)&=[(f(0)\wedge\bar{x})\vee(f(1)\wedge x)]\wedge[(g(0)\wedge\bar{x})\vee(g(1)\wedge x)]\\
&=(f(0)\wedge g(0)\wedge\bar{x})\vee(f(1)\wedge g(1)\wedge x)。
\end{aligned}
$$

由于每个表达式都是由补、并、交构成的，因此对于任何单变量的布尔函数 $f(x)$，(7-1) 式成立。

假设 (7-15) 式对 r 个变量的布尔函数是成立的，我们证明它对 $r+1$ 个变量的布尔函数也成立。

$$
\begin{aligned}
f(x_1, x_2, \cdots, x_r, x_{r+1}) &= (f(x_1, x_2, \cdots, x_r, 0) \wedge \bar{x}_{r+1}) \vee (f(x_1, x_2, \\
&\qquad \cdots, x_r, 1) \wedge x_{r+1}) \\
&= [(\vee_{\delta_1\delta_2\cdots\delta_r = 00\cdots0}^{11\cdots1}(f(\delta_1, \delta_2, \cdots, \delta_r, 0) \wedge m_{\delta_1\delta_2\cdots\delta_r})) \wedge \bar{x}_{r+1}] \\
&\quad \vee [(\vee_{\delta_1\delta_2\cdots\delta_r = 00\cdots0}^{11\cdots1}(f(\delta_1, \delta_2, \cdots, \delta_r, 1) \wedge m_{\delta_1\delta_2\cdots\delta_r})) \wedge x_{r+1}] \\
&= \vee_{\delta_1\delta_2\cdots\delta_{r+1} = 00\cdots0}^{11\cdots1}(f(\delta_1, \delta_2, \cdots, \delta_r, \delta_{r+1}) \wedge m_{\delta_1\delta_2\cdots\delta_{r+1}}) \\
&= \vee_{k=00\cdots0}^{11\cdots1}(c_k \wedge m_k).
\end{aligned}
$$

(这里 k 取 $0—2^{r+1}-1$ 的所有十进制数的二进制表示). 证完.

上述定理说明 $\langle B; -, \vee, \wedge \rangle$ 上的每一布尔表达式都能表示为所有最小项的加"权"并或所有最大项的加"权"交。这里的"权"是指 $C_{\delta_1\delta_2\cdots\delta_n}$, 即 $f(\delta_1, \delta_2, \cdots, \delta_n)$ 乃是 B 中的元素，这两种形式分别叫做布尔表达式的**最小项标准形式**和**最大项标准形式**。因为"权"是唯一的，故这两种标准形式也是唯一的。

例 2 对例 1 中的布尔表达式

$$f(x, y) = (\beta \wedge \bar{x} \wedge y) \vee (\beta \wedge x \wedge (\overline{x \vee \bar{y}})) \vee (\alpha \wedge (x \vee (\bar{x} \wedge y)))$$

运用表 7-7，可写出其最小项标准形式和最大项标准形式如下：

$$
\begin{aligned}
f(x, y) &= (c_{00} \wedge m_{00}) \vee (c_{01} \wedge m_{01}) \vee (c_{10} \wedge m_{10}) \vee (c_{11} \wedge m_{11}) \\
&= (f(0,0) \wedge \bar{x} \wedge \bar{y}) \vee (f(0,1) \wedge \bar{x} \wedge y) \vee (f(1,0) \wedge x \wedge \bar{y}) \\
&\quad \vee (f(1,1) \wedge x \wedge y) \\
&= (0 \wedge \bar{x} \wedge \bar{y}) \vee (1 \wedge \bar{x} \wedge y) \vee (\alpha \wedge x \wedge \bar{y}) \vee (\alpha \wedge x \wedge y), \\
f(x, y) &= (c_{00} \vee \widetilde{m}_{00}) \wedge (c_{01} \vee \widetilde{m}_{01}) \wedge (c_{10} \vee \widetilde{m}_{10}) \wedge (c_{11} \vee \widetilde{m}_{11}) \\
&= (f(0,0) \vee x \vee y) \wedge (f(0,1) \vee x \vee \bar{y}) \wedge (f(1,0) \vee \bar{x} \vee y) \\
&\quad \wedge (f(1,1) \vee \bar{x} \vee \bar{y}) \\
&= (0 \vee x \vee y) \wedge (1 \vee x \vee \bar{y}) \wedge (\alpha \vee \bar{x} \vee y) \wedge (\alpha \vee \bar{x} \vee \bar{y}).
\end{aligned}
$$

显然，由 $A_1, A_2, \cdots, A$ 产生的集合 (§1.4) 可看作是在布尔

代数〈$\{\Phi, U\}$; ′, ∪, ∩〉上由 $A_1, A_2, \cdots, A_r$ 产生的布尔表达式。§1.9导出的它们的最小集标准形式和最大集标准形式不过是定理7-33中“权”为 Φ 或 U 的特殊情形。

布尔表达式的标准形式还能由类似于算法1-3，1-4的方法而得到。下面仅举例加以说明。

例如，例2中的布尔表达式 $f(x,y)$ 的最小项标准形式和最大项标准形式可如下求得。

$$
\begin{aligned}
f(x,y) &= (\beta\wedge\bar{x}\wedge y)\vee(\beta\wedge x\wedge(\overline{x\vee\bar{y}}))\vee(\alpha\wedge(x\vee(\bar{x}\wedge y)))\\
&= (\beta\wedge\bar{x}\wedge y)\vee(\beta\wedge x\wedge\bar{x}\wedge y)\vee(\alpha\wedge x)\vee(\alpha\wedge\bar{x}\wedge y)\\
&= (\bar{x}\wedge y)\vee(\alpha\wedge x)\\
&= (\bar{x}\wedge y)\vee(\alpha\wedge x\wedge y)\vee(\alpha\wedge x\wedge\bar{y})\\
&= (0\wedge\bar{x}\wedge\bar{y})\vee(1\wedge\bar{x}\wedge y)\vee(\alpha\wedge x\wedge\bar{y})\vee(\alpha\wedge x\wedge y).
\end{aligned}
$$

$$
\begin{aligned}
f(x,y) &= (\beta\wedge\bar{x}\wedge y)\vee(\beta\wedge x\wedge(\overline{x\vee\bar{y}}))\vee(\alpha\wedge(x\vee(\bar{x}\wedge y)))\\
&= (\bar{x}\wedge y)\vee(\alpha\wedge x)\\
&= (\alpha\vee\bar{x})\wedge(\alpha\vee y)\wedge(x\vee y)\\
&= (\alpha\vee\bar{x}\vee y)\wedge(\alpha\vee\bar{x}\vee\bar{y})\wedge(\alpha\vee x\vee y)\wedge(x\vee y)\\
&= (0\vee x\vee y)\wedge(\alpha\vee\bar{x}\vee y)\wedge(\alpha\vee\bar{x}\vee\bar{y})\\
&= (0\vee x\vee y)\wedge(1\vee x\vee\bar{y})\wedge(\alpha\vee\bar{x}\vee y)\wedge(\alpha\vee\bar{x}\vee\bar{y}).
\end{aligned}
$$

因为〈B; $-$, ∨, ∧〉上的布尔函数 $f(x_1, x_2, \cdots, x_n)$ 是由它的 2^n 个“权”唯一确定的，而每一个“权”都是 B 的元素。于是〈B; $-$, ∨, ∧〉上存在 $(\# B)^{2^n}$ 个不同的布尔函数。另一方面，不同的形如 $f: B^n \to B$ 的函数的数目等于 $(\# B)^{(\# B)^n}$。因此，当 $\# B > 2$ 时，一定有不是布尔函数的形如 $f: B^n \to B$ 的函数存在。

例如，函数 $f: B^2 \to B$，其中 $B = \{0, \alpha, \beta, 1\}$，$f(0,0) = 0$，

$$f(0,1) = 1,\ f(1,0) = f(1,1) = \alpha,\ f(0,\alpha) = \beta.$$

f 不是一个布尔函数。因为若 f 是布尔函数，则

$$
\begin{aligned}
f(x,y) &= (0\wedge\bar{x}\wedge\bar{y})\vee(1\wedge\bar{x}\wedge y)\vee(\alpha\wedge x\wedge\bar{y})\vee(\alpha\wedge x\wedge y)\\
&= (\bar{x}\wedge y)\vee(\alpha\wedge x\wedge\bar{y})\vee(\alpha\wedge x\wedge y).
\end{aligned}
$$

将 $x=0$，$y=\alpha$ 代入上式，得

$$f(0,\alpha)=\alpha\vee 0\vee 0=\alpha\neq\beta.$$

所以，上一函数不是布尔函数。

习　　题

1. 下列各集合对于整除关系|都构成偏序集。在每个集合中对存在有最大下界和最小上界的元素对，找出它们的最大下界和最小上界；指出各集合中是否有最小元素和最大元素。

(1) $L=\{1,2,3,4,6,12\}$，

(2) $L=\{1,2,3,4,6,8,12,24\}$，

(3) $L=\{1,2,3,\cdots,12\}$。

2. 设 $\langle L_1;\leqslant\rangle$ 和 $\langle L_2;\leqslant\rangle$ 是偏序集，按下面方式定义 $L_1\times L_2$ 上的关系 $\leqslant$：对于所有的 $(l_1,l_2),(l_1',l_2')\in L_1\times L_2$，有

$$((l_1,l_2)\leqslant(l_1',l_2'))\Longleftrightarrow(l_1\leqslant l_1',\ l_2\leqslant l_2').$$

试证明 $\langle L_1\times L_2;\leqslant\rangle$ 是偏序集。

3. 试证明在格中如果有 $a\leqslant b$ 和 $c\leqslant d$，则有

$$a\wedge c\leqslant b\wedge d \text{ 且 } a\vee c\leqslant b\vee d.$$

4. 试证明在格中对于任意元素 a,b,c,d，有

$$(a\wedge b)\vee(c\wedge d)\leqslant(a\vee c)\wedge(b\vee d).$$

5. 在第1题中，哪一个偏序集构成格？

6. 试证明若 $\langle L;\vee,\wedge\rangle$ 是有限格，则 L 一定有最小元素和最大元素。

7. 图 7-9 给出了三个偏序集的次序图，其中哪些构成格？

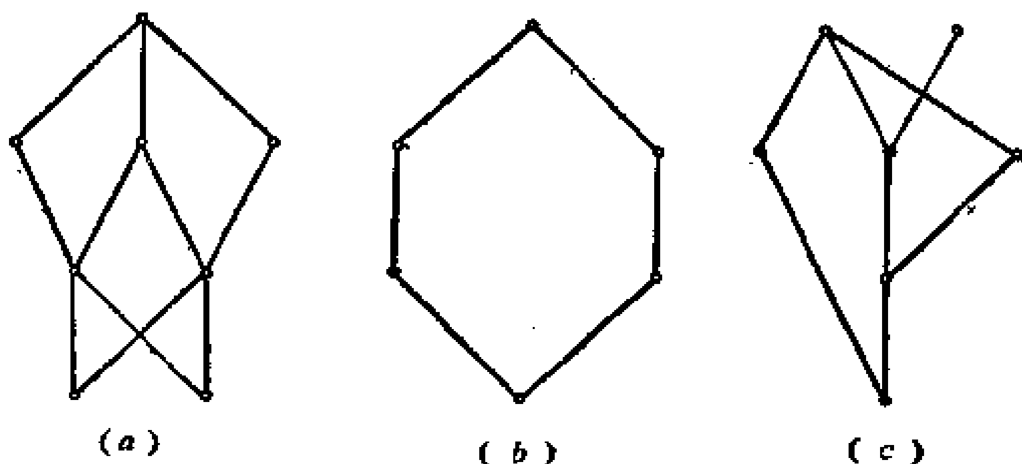


图 7-9

8. 设 $\langle L; \vee, \wedge\rangle$ 是格，试证明对于所有的 $a, b, c \in L$，有

$$(a \leqslant b) \Rightarrow (a \vee (b \wedge c) \leqslant b \wedge (a \vee c))。$$

9. 设 $\langle L; \vee, \wedge\rangle$ 是一个格，如果对于所有的 $a, b, c \in L$，有

$$(a \leqslant b) \Rightarrow (a \vee (b \wedge c) = b \wedge (a \vee c)),$$

则称 $\langle L; \vee, \wedge\rangle$ 是模式格。图 7-10 所给出的格是模式格吗？证明你的结论。

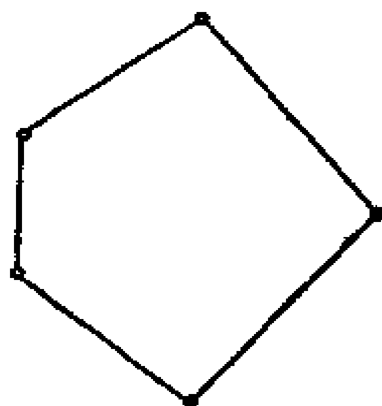


图 7-10

10. 试证明每一个分配格都是模式格，但模式格却不一定是分配格。

11. 链 $\langle L; \leqslant\rangle$ 是一个偏序集，对于任意的 $l_1, l_2 \in L$，或者 $l_1 \leqslant l_2$，或者 $l_2 \leqslant l_1$。试证明每一个链都形成一个分配格。

12. 试证明在具有两个或更多个元素的格中，不会有元素是它自身的补。

13. 试证明具有三个或更多个元素的链不是有补格。

14. 设 $\langle L; \vee, \wedge\rangle$ 是一个格，$\# L > 1$，试证明如果 $\langle L; \vee, \wedge\rangle$ 有元素 1 和元素 0，则这两个元素必定是不相同的。

15. 试举例说明并非每一有补格都是分配格；并非每一分配格都是有补格。

16. 考察代数系统 $\langle F; -, \vee, \wedge\rangle$，这里 $F=\{f \mid f: N\to\{0,1\}\}$，对于任意的 $f_1, f_2\in F$，

当且仅当 $f_1(n)=0$ 时，$\bar{f}_1(n)=1$；

当且仅当 $f_1(n)=1$ 或 $f_2(n)=1$ 时，$(f_1\vee f_2)(n)=1$；

当且仅当 $f_1(n)=1$ 且 $f_2(n)=1$ 时，$(f_1\wedge f_2)(n)=1$；

试证明 $\langle F; -, \vee, \wedge\rangle$ 是布尔代数。

17. 设 $A_1, A_2, \cdots, A_r$ 是全集合 U 的任意子集。S 是由 $A_1, A_2, \cdots, A_r$ 产生的所有集合的集合，试证明 $\langle S; ', \cup, \cap\rangle$ 是布尔代数。

18. 不用定理 7-31，证明不存在其域的基数为 3 的布尔代数。

19. 设 $U=\{u_1, u_2, u_3, u_4\}$，证明代数系统 $W=\langle\{\phi, \{u_1, u_2\}, \{u_3, u_4\}, U\}; ', \cup, \cap\rangle$ 是布尔代数。W 的原子的集合 M 是什么？画出 W 和布尔代数 $\langle 2^M; ', \cup, \cap\rangle$ 的次序图。

20. 代数系统 $\langle A; ', +, \cdot\rangle$ 中 $A=\{\alpha, \beta, \gamma, \delta\}$，其运算定义如下：

a	a'
α	δ
β	γ
γ	β
δ	α

$+$	α	β	γ	δ
α	α	α	γ	γ
β	α	β	γ	δ
γ	γ	γ	γ	γ
δ	γ	δ	γ	δ

$\cdot$	α	β	γ	δ
α	α	β	α	β
β	β	β	β	β
γ	α	β	γ	δ
δ	β	β	δ	δ

这个系统是布尔代数吗？证明你的结论。

21. 下面是布尔代数 $\langle\{0, \alpha, \beta, 1\}; -, \vee, \wedge\rangle$ 上由 x, y 产生的布尔表达式

$$f(x, y)=(x\wedge(\alpha\vee y))\vee(\bar{x}\wedge\bar{y}),$$

列出对于所有自变量 $(x, y)\in B^2$ 的 $f(x, y)$ 之值的表。

22. 利用第21题建立的表直接写出第21题中 $f(x, y)$ 的最小项和最大项标准形式。

23. 下面是布尔代数$\langle\{0,\alpha,\beta,1\};-,\vee,\wedge\rangle$上由$x,y,z$产生的布尔表达式

$$f(x,y,z)=(\overline{(\beta\wedge\bar{x})\vee(y\wedge(\alpha\vee\bar{z}))})\vee(\bar{y}\wedge\bar{z}),$$

用类似于算法1-3和算法1-4的方法，求此表达式的最小项和最大项标准形式。

24. 设$\langle L;\leqslant\rangle$是一个格，试证明对于任意的元素$a,b,c\in L$，有下列命题成立：

(1) 若$a\wedge b=a\vee b$，则$a=b$；

(2) 若$a\wedge b\wedge c=a\vee b\vee c$，则$a=b=c$；

(3) $a\vee[(a\vee b)\wedge(a\vee c)]=(a\vee b)\wedge(a\vee c)$。

25. 设a和b是格$\langle L;\leqslant\rangle$中的两个元素，试证明当且仅当$a$和$b$是不可比时，有$a\wedge b<a$和$a\wedge b<b$。

26. 设集合$A=\{a,b,c\}$，集合A上所有分划所构成的集合为$\mathbf{P}(A)$。你能否适当定义$\mathbf{P}(A)$上一个偏序关系"$\leqslant$"，使得$\langle P(A);\leqslant\rangle$成为一个格？

27. 试证明在格中对于任意元素a,b,c，有

$(a\wedge b)\vee(b\wedge c)\vee(c\wedge a)\leqslant(a\vee b)\wedge(b\vee c)\wedge(c\vee a)$。

28. 试证明当且仅当对于任意元素$a,b,c\in L$，有$(a\wedge b)\vee(b\wedge c)\vee(c\wedge a)=(a\vee b)\wedge(b\vee c)\wedge(c\vee a)$时，格$\langle L;\leqslant\rangle$是可分配格。

(提示：要证明$\langle L;\leqslant\rangle$是分配格，可考虑元素$(a\vee b)\wedge(a\vee c)$，$b\vee c$及$a$)

29. 设$\langle B;-,\vee,\wedge\rangle$是一布尔代数，试证明$\langle B;\oplus\rangle$是一个交换群，这里$\oplus$定义为

$$a\oplus b=(a\wedge\bar{b})\vee(\bar{a}\wedge b)。$$

第八章 图 论

在第二章讨论关系图时，我们已经提到过图论的一些概念，在那里，图只是作为表达一个集合上二元关系的一种手段。在这一章，我们要将图的概念一般化。

图论是建立和处理离散数学模型的一个重要工具，是一门应用性很强的学科，例如在社会科学、语言学、计算机科学、物理学、化学、信息论、控制论以及经济管理等各个方面都有着广泛的应用。图论在计算机科学的许多领域中，例如在开关理论与逻辑设计、数据结构、形式语言、操作系统、编译程序的编写以及信息的组织与检索中均起着重要的作用。

本章首先介绍图论的一些基本概念和基本性质，然后介绍几种在实际应用中有着重要意义的特殊图。

§8.1 基本概念

定义 8-1 一个图G是一个有序二元组 (V,E)，记作$G=(V,E)$，其中

(1) $V=\{v_1,v_2,\cdots,v_n\}$ 是一个有限非空的集合，V的元素称为G的**结点**（或顶点），V称为G的**结点集**；

(2) E是V中不同元素的非有序对偶（即形如 $\{v_i,v_j\}$，其中$v_i\neq v_j$）的集合，这些对偶称为G的**边**（或弧），而E称为G的**边集**。

一个图可以用平面上的一个图解来表示，用平面上的一些点代表图的结点，图的边用连接相应结点而不经过其他结点的直线

(或曲线) 来代表。由于结点位置的选取和边的形状的任意性，一个图可以有各种在外形上看起来差别很大的图解。我们经常将图的一个图解就看作是这个图。

例如，设 $V=\{v_1,v_2,v_3,v_4,v_5\}$，$E=\{\{v_1,v_2\},\{v_1,v_3\},\{v_2,v_3\},\{v_2,v_4\},\{v_3,v_5\},\{v_4,v_5\}\}$，图 $G=(V,E)$ 的图解可以分别画成如图 8-1 的 (a)，(b)，(c)的样子。

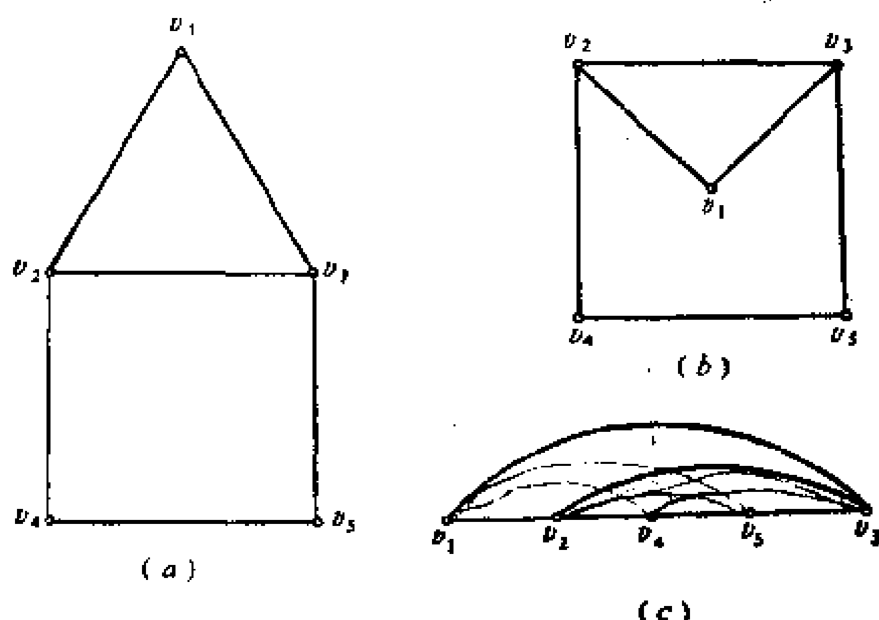


图 8-1

具有 n 个结点和 m 条边的图称为 **(n,m) 图**。$(n,0)$ 图称为**零图**。$(1,0)$ 图称为**平凡图**。

如果 $e=\{v_i,v_j\}$ 是 G 的边，则称结点 v_i 和 v_j 是**邻接的**，e 和 v_i 以及 e 和 v_j 均称为是**关联的**。没有边关联于它的结点称为是**孤立点**。关联于同一结点的相异边称为是**邻接的**。不与其它任何边相邻接的边称为是**孤立边**。例如图 8-1 中 v_2和 v_3、v_1 和 v_2 分别是相互邻接的结点。边 $\{v_1,v_3\}$ 关联于 v_3，边 $\{v_2,v_3\}$、$\{v_3,v_5\}$ 也关联于 v_3，因此边 $\{v_1,v_3\}$、$\{v_2,v_3\}$ 和 $\{v_3,v_5\}$ 是相互邻接的。

定义 8-2 在图G中，如果任意两个不同的结点都是邻接的，

则称图G是**完全图**。

例如，图 8-2 就是一个具有五个结点的完全图。在一个完全的 (n,m) 图中，$m=C_n^2=\frac{n(n-1)}{2}$。

定义 8-3 图G的**补图**是由G的所有结点和为了使G成为完全图所需要添加的那些边所组成的图，用 $\bar{G}$ 表示。

例如，图 8-3 是图 8-1 的补图。显然，若 $\bar{G}$ 是G的补图，则G也是 $\bar{G}$ 的补图。

图G中关联于结点 v_i 的边的总数称为结点 v_i 的**次数**，用 $\deg(v_i)$ 表示。例如，图 8-1 中结点 v_1、v_2、v_3、v_4 和 v_5 的次数分别为 2、3、3、2 和 2。

由于每条边关联于两个结点，因此图G的所有结点的次数的总和为边数的二倍。于是，若G为具有结点集 $\{v_1, v_2, \cdots, v_n\}$ 的 (n,m) 图，则

$$\sum_{i=1}^{n}\deg(v_i)=2m.$$

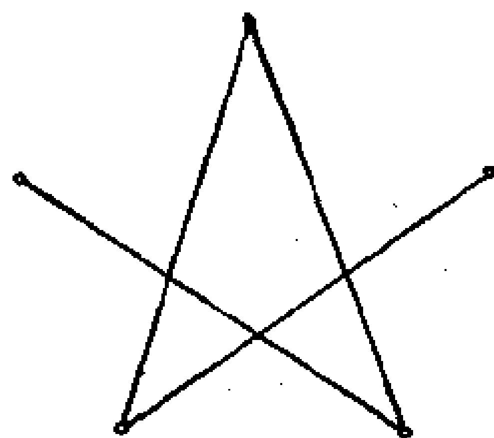


图 8-2

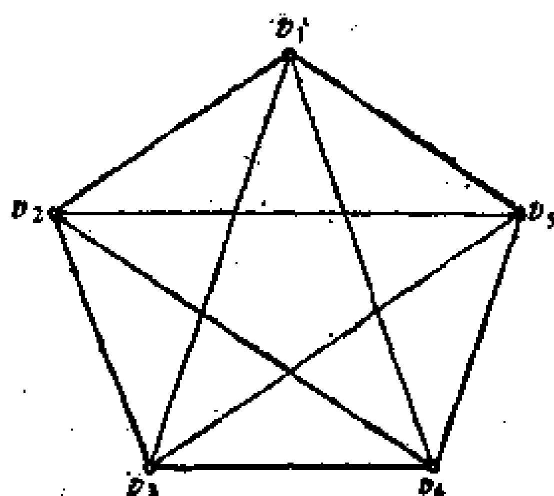


图 8-3

定义 8-4 若图G的所有结点都具有同一次数 d，则称图G为**d 次正则图**。

图 8-4 是一个 3 次正则图。

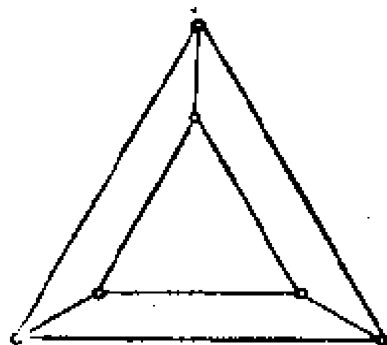


图 8-4

定义 8-5 设G和G'是两个分别具有结点集V和V'的图，若存在一个双射$h: V \to V'$，使得当且仅当$\{v_i, v_j\}$是G中的边时，$\{h(v_i), h(v_j)\}$是G'中的边，则称G'**同构于**G。

显然，若G'同构于G，则G亦同构于G'。因此可简单地称G和G'**同构**。图 8-5 给出了两个同构的图，其中同构h由$h(v_i)=v'_i\ (i=1,2,\cdots,6)$给出。由于同构的图除了它们的结点标记可能不一样外，其他是完全相同的。因此，任何对于图G成立的结论，对于同构于G的图也是成立的。

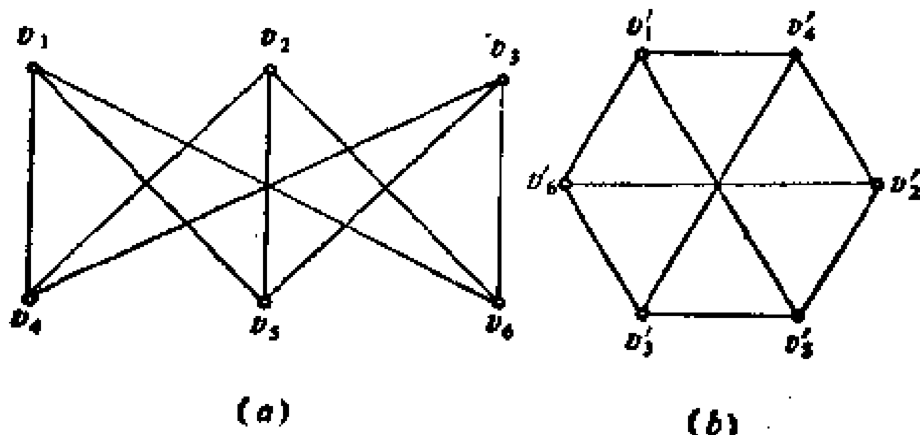


图 8-5

定义 8-6 设有图$G=(V,E)$和图$\tilde{G}=(\tilde{V},\tilde{E})$，

1. 若$\tilde{V}\subseteq V$，$\tilde{E}\subseteq E$，则称$\tilde{G}$是G的**子图**；
2. 若$\tilde{V}\subseteq V$，$\tilde{E}\subseteq E$，且$\tilde{E}\neq E$，则称$\tilde{G}$是G的**真子图**；
3. 若$\tilde{V}=V$，$\tilde{E}\subseteq E$，则称$\tilde{G}$是G的**生成子图**。

显然，任一图G都是自己的子图。又如，图 8-3 是图 8-2 的生成子图，也是真子图。

图G中 l 条边的序列 $\{v_{i_0}, v_{i_1}\}$, $\{v_{i_1}, v_{i_2}\}$, …, $\{v_{i_{l-1}}, v_{i_l}\}$ 称为连接 v_{i_0} 到 v_{i_l} 的长度为 l 的**路**。它也可以表示为 $\{v_{i_0}, v_{i_1}\}\{v_{i_1}, v_{i_2}\}\cdots\{v_{i_{l-1}}, v_{i_l}\}$，或更简单地表示为 $v_{i_0}v_{i_1}\cdots v_{i_l}$。若 $v_{i_0}\neq v_{i_l}$，则路 $v_{i_0}v_{i_1}\cdots v_{i_l}$ 称为**开路**。若 $v_{i_0}=v_{i_l}$，则称为**回路**。若 $v_{i_0}, v_{i_1}, \cdots, v_{i_l}$ 各不相同，则称开路 $v_{i_0}v_{i_1}\cdots v_{i_l}$ 为**真路**。若 $v_{i_0}, v_{i_1}, \cdots, v_{i_{l-1}}$ 各不相同，则称回路 $v_{i_0}v_{i_1}\cdots v_{i_{l-1}}v_{i_0}$ 为**环**。(但形为 $v_iv_jv_i$ 的回路不能称作环)。

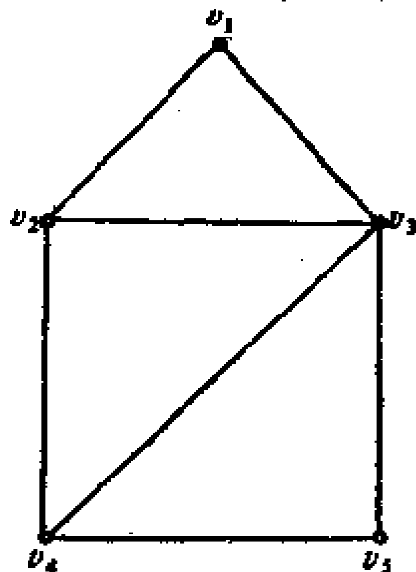


图 8-6

在图 8-6 中，$v_1v_2v_4v_6$ 是一条长为 3 的开路，也是一条真路。$v_1v_2v_3v_5v_4v_2$ 是一条开路，但不是真路。$v_1v_3v_2v_4v_5v_3v_1$ 是一条长为 6 的回路，但不是环。$v_1v_3v_2v_1$ 是一条回路，也是环。

在图G中，若存在一条路连接 v_i 和 v_j，则称该图中的两个结点 v_i 与 v_j 是**连接的**。

定义 8-7 若图G中，任意两个结点均是连接的，则称图G是**连通的**，否则是**不连通的**。

例如，图 8-6 是连通的，但图 8-7 是不连通的。



图 8-7

若图G的子图H具有某一性质P，而其他所有包含子图H的子图不具有性质P，则称H为G的具有性质P的极大子图。图G的极大连通子图称为G的**分图**。

例如，图 8-8 给出了一个具有六个分图的图。

图G的**分离边** $\{v_i, v_j\}$ 是这样的边，若去掉该边，则和 v_i 相连接的结点集与和 v_j 相连接的结点集的交为空。于是，若从图G中去掉一条分离边 e，必然将包含边 e 的图G的分图分成两个分图（参见图 8-9）。显然，G 中的任何边，若其不是分离边，则必出现于G的某个环中。

在图G中，从结点 v_i 到 v_j 若由一条或更多条路相连接，则其中必有长度最短的路，称其为从 v_i 到 v_j 的**短程**。

例如图 8-10 中，从 v_1 到 v_5 的短程是 $v_1v_2v_5$。从 v_2 到 v_3 的短程是 $v_2v_1v_3$ 或 $v_2v_4v_3$。

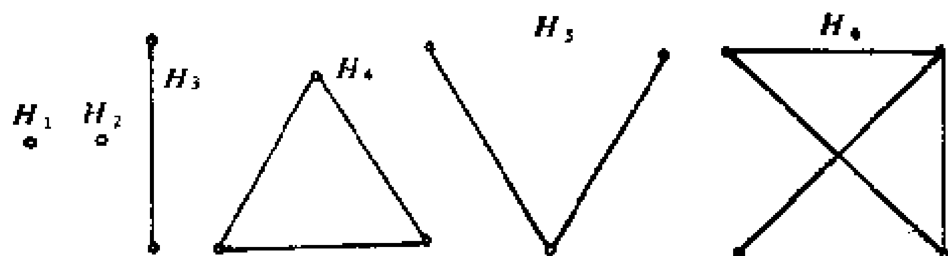


图 8-8

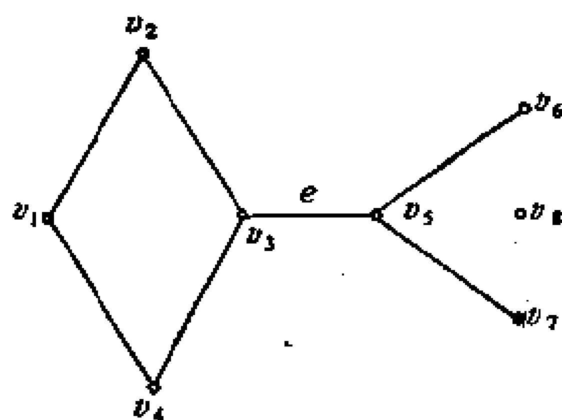


图 8-9

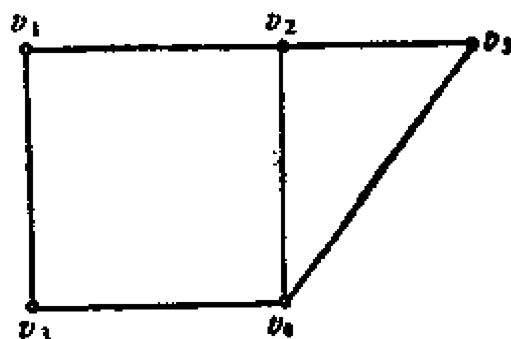


图 8-10

定理 8-1 设G是具有结点集 $V=\{v_1, v_2, \cdots, v_n\}$ 的图，则对于任意两个相连接的结点 v_i，$v_j \in V$ $(v_i \neq v_j)$，其短程是一条长度不大于 $n-1$ 的真路。

证明 设α为任一连接v_i到v_j的路，且

$$\alpha = v_i v_{i_1} v_{i_2} \cdots v_{i_{l-1}} v_j.$$

若α中有相同的结点，设为$v_{i_r} = v_{i_k}$ $(r<k)$，则子路$v_{i_{r+1}}\cdots v_{i_k}$可以从$\alpha$中删去而形成一条较短的路$\beta = v_i v_{i_1}\cdots v_{i_r} v_{i_{k+1}}\cdots v_{i_{l-1}} v_j$连接$v_i$到$v_j$。若$\beta$中还有相同的结点，那么重复上述过程可形成一条更短的路。这样，最后必得到一条真路，它连接v_i到v_j，并且短于前述任一非真的路，因此，只有真路才能是短程。然而在任一长度为l的真路$v_i v_{i_1} v_{i_2}\cdots v_{i_{l-1}} v_j$中，其结点$v_i, v_{i_1}, \cdots, v_{i_{l-1}}, v_j$是各不相同的，这就意味着$l+1 \leqslant n$，即路长$l \leqslant n-1$。定理得证。

从v_i到v_j的短程的长度称为v_i和v_j间的**距离**，用$d(v_i, v_j)$来表示。因此，在n个结点的图中任意两个相连接的结点间的距离$d(v_i, v_j) \leqslant n-1$。对于任一结点$v_i$，假定$d(v_i, v_i) = 0$。

推论 设G是具有n个结点的图，则G中任一环的长度不大于n。

图的概念能从多方面加以推广。

设$G=(V,E)$，V是一个有限非空的集合，E是V中任意元素的非有序对偶的多重集，则称G是一个**伪图**。

注意，伪图和前面所定义的图的区别是：首先，在E中允许出现相同元素的对偶，即对于元素$v \in V$，可能有$\{v, v\} \in E$。第二，E是一个多重集，即对于元素v_i，$v_j \in V$，在E中无序对偶$\{v_i, v_j\}$可能出现r次，$r>1$。例如，设$V=\{v_1, v_2, v_3, v_4\}$，$E=\{\{v_1,v_2\},\{v_1,v_2\},\{v_1,v_4\},\{v_2,v_4\},\{v_4,v_4\},\{v_3,v_3\}\}$，$G=(V,E)$就是一伪图。伪图也可用平面上图解的方法来表示，若无序对偶$\{v_i, v_j\}$在E中出现r次，则在结点v_i和v_j之间连接r条直线(或曲线)，若在E中有对偶$\{v_i, v_i\}$出现，则绕顶点v_i画一长度为1的环。图8-11就是上例中伪图的图解表示。

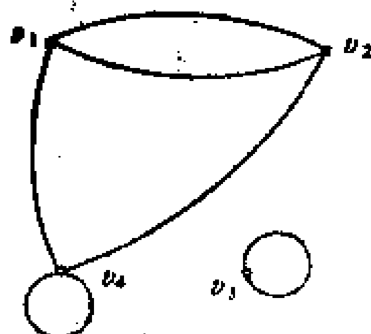


图8-11

没有长度为 1 的环的伪图称为**多重图**。图8-12给出了一多重图的例。相对于伪图，我们将本节开始定义的图称为**简单图**。它既没有多重边，也没有长度为 1 的环。

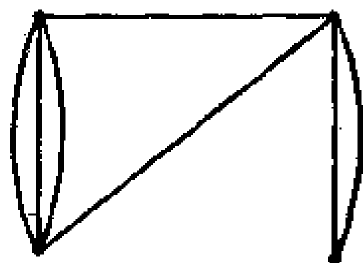


图 8-12

设 $G=(V,E)$，V是一有限非空集合，E是V中不同元素的有序对偶的集合，则称G是一**有向图**。在有向图中，对于$v_i \neq v_j$，(v_i,v_j)和(v_j,v_i)是两条不同的边。在有向图的图解中，用一个从结点v_i指向v_j的箭头表示边(v_i,v_j)。相应地，用从结点v_j指向v_i的箭头表示边(v_j,v_i)。

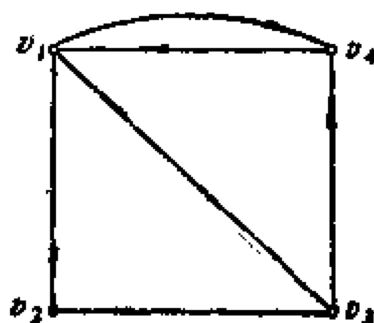
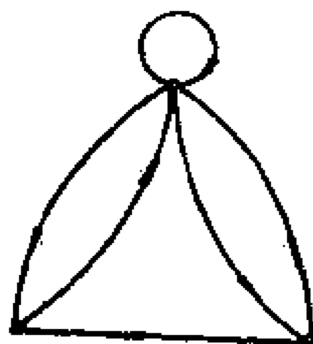


图 8-13

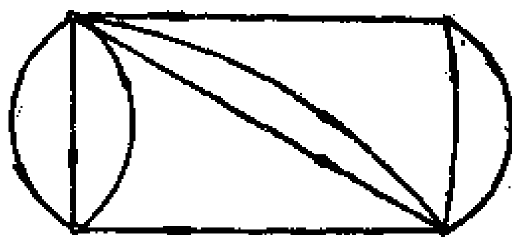
图 8-13 给出了有向图的例。

相对于有向图，我们分别称前面所定义的图为**无向图**、**无向伪图**和**无向多重图**。

用类似的方法也可以定义**有向伪图**和**有向多重图**。图 8-14 给出了有向伪图和有向多重图的例。



有向伪图



有向多重图

图 8-14

对于多重图，我们也可采用在边上附加数字表示边的相重次

数的方法来表示。例如，图 8-12 中的无向多重图又可用图 8-15 表示。图 8-14 中的有向多重图，又可用图 8-16 表示。

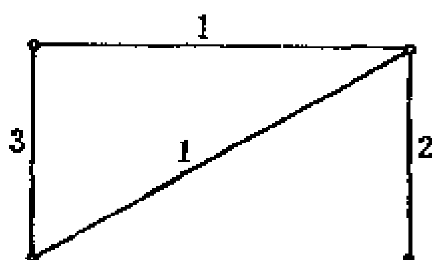


图 8-15

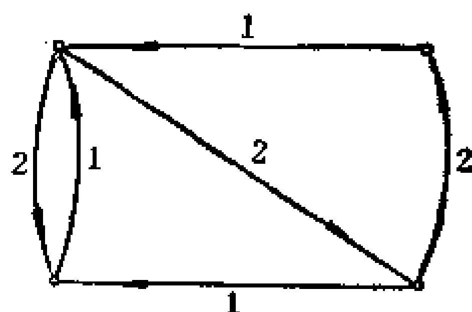


图 8-16

每一条边的相重次数可以看作该边的权。更一般地，权可以不一定是整数。如图 8-17 所示。

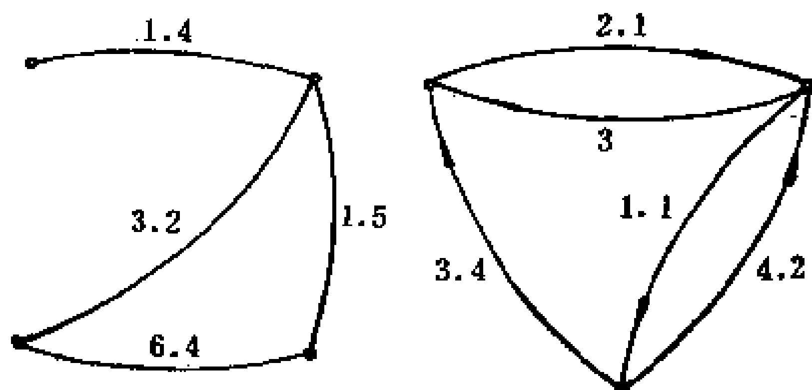


图 8-17

给每一条边都指定了权的图称为**有权图**。将一个物理状态模拟为一个抽象图时，在许多场合，都希望把附加信息放到图的边上。例如，在一个表示城市间的公路连接的图中，我们可以给每一条边指定一个数，表示用该边连结的两个城市间的距离。又如在表示输油管系统的图中，所指定的权可以用来表示单位时间内流过输油管的油量。有权图可定义为一个有序三元组 (V, E, f)，这里 V 是结点集，E 是边集，f 是一个函数，它的定义域是 E，通过函数 f 将权分配给各边。下面我们主要讨论无向图，当不作特别声明时，所谓“图”即指简单无向图。

§8.2 图的矩阵表示

前面给出了图的图解表示，它对于分析给定图的某些特性有时是有用的，但当图中的结点和边的数目较大时，这种办法是不实际的。表示图的另一个方便的方法是用相应的邻接矩阵。这种表示方法有许多优点，它使得图的有关信息能以矩阵的形式在计算机中储存起来并加以变换，利用矩阵的表示及其运算还可以得到图的一些有关性质。然而也应该看到，图的许多有强烈的直观背景的性质，在用矩阵的语言表述时会遇到困难。例如关于平面性的问题就是如此。

定义 8-8 设图 $G=(V,E)$，其中 $V=\{v_1,v_2,\cdots,v_n\}$，n 阶方阵 $A=(a_{ij})$ 称为 G 的**邻接矩阵**，其中元素

$$a_{ij}=\begin{cases}1 & 若\ \{v_i,v_j\}\in E;\\ 0 & 否则。\end{cases}$$

例如，图 8-1 的邻接矩阵是

$$A=\begin{matrix} & v_1 & v_2 & v_3 & v_4 & v_5 \\ v_1 & 0 & 1 & 1 & 0 & 0 \\ v_2 & 1 & 0 & 1 & 1 & 0 \\ v_3 & 1 & 1 & 0 & 0 & 1 \\ v_4 & 0 & 1 & 0 & 0 & 1 \\ v_5 & 0 & 0 & 1 & 1 & 0 \end{matrix}.$$

由定义可见，一个图的邻接矩阵是对角线元素均为零的对称 0-1 矩阵。反之，若给定任何对角线元素均为零的对称 0-1 矩阵 A，显然可以唯一地作一个图 G，以 A 为邻接矩阵。当然，邻接矩阵依赖于 V 中各元素的给定次序，对于 V 中各元素的不同给定次序，可以得到同一个图 G 的不同的邻接矩阵。但是，G 的任何

一个邻接矩阵，都可以由G的另一个邻接矩阵通过交换某些行和相应的列而得到。我们将不考虑这种由于V中元素的给定次序而引起的邻接矩阵的任意性，并选取给定图的任何一个邻接矩阵作为该图的邻接矩阵。事实上，如果两个图有这样的邻接矩阵，其中的一个可通过另一个交换某些行和相应的列而得到，则这两个图是同构的。

显然，图G的邻接矩阵A的第i行（或第i列）出现的1的个数即为结点v_i的次数。又图G的邻接矩阵A的(i,j)项元素a_{ij}实际上给出了从v_i到v_j的长度为1的路的数目。这个事实是下面定理的一种特殊情形。

定理 8-2 设G是具有结点集$\{v_1, v_2, \cdots, v_n\}$和邻接矩阵$A$的图，则$A^l(l=1,2,3,\cdots)$的$(i,j)$项元素$a_{ij}^{(l)}$是连接$v_i$到$v_j$的长度为$l$的路的总数。

证明 （对l进行归纳）当$l=1$时，$A^1=A$，由A的定义，定理显然成立。

设$a_{ij}^{(l)}$表示A^l的(i,j)项，并假设定理对l是成立的，由于$A^{l+1}=A^l \cdot A$，因此有$a_{ij}^{(l+1)}=\sum_{k=1}^{n} a_{ik}^{(l)} a_{kj}$。由归纳假设可知，$a_{ik}^{(l)} a_{kj}$是以$v_k$作为倒数第二个结点连接$v_i$到$v_j$的长度为$l+1$的路的数目。对所有的$k$求和，即得$a_{ij}^{(l+1)}$是以任意结点为倒数第二个结点连接$v_i$到$v_j$的长度为$l+1$的路的总数。于是定理对$l+1$也成立，因此定理得证。

由定理8-1和定理8-2，我们可以得到如下结论：

(1) 如果对$l=1,2,\cdots,n-1$，A^l的(i,j)项元素$(i \neq j)$都为0，那末v_i和v_j之间无任何路相连结（因此，v_i和v_j必然属于G的不同的分图）；

(2) 结点v_i和$v_j (i \neq j)$之间的距离$d(v_i, v_j)$是使A^l的(i, j)项元素不为零的最小正整数l。

例 1 具有结点集$\{v_1, v_2, v_3, v_4, v_5, v_6\}$的图$G$的邻接矩阵为

$$A=\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \end{pmatrix},$$

由矩阵的乘法运算，我们得到：

$$A^2=\begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 1 & 1 \\ 0 & 0 & 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 1 & 1 & 2 \end{pmatrix}, \quad A^3=\begin{pmatrix} 0 & 2 & 0 & 0 & 0 & 0 \\ 2 & 0 & 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 3 & 3 \\ 0 & 0 & 0 & 3 & 2 & 3 \\ 0 & 0 & 0 & 3 & 3 & 2 \end{pmatrix},$$

$$A^4=\begin{pmatrix} 2 & 0 & 2 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 & 0 & 0 \\ 2 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 6 & 5 & 5 \\ 0 & 0 & 0 & 5 & 6 & 5 \\ 0 & 0 & 0 & 5 & 5 & 6 \end{pmatrix}, \quad A^5=\begin{pmatrix} 0 & 4 & 0 & 0 & 0 & 0 \\ 4 & 0 & 4 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 10 & 11 & 11 \\ 0 & 0 & 0 & 11 & 10 & 11 \\ 0 & 0 & 0 & 11 & 11 & 10 \end{pmatrix}.$$

由这些矩阵我们可以看到，例如，v_1 到v_2有两条长为 3 的路相连接；v_3 和 v_4 之间没有长度 $\leqslant 5$ 的路相连接，因此v_3 和 v_4 属于G的两个不同的分图；v_4 到 v_4 有两条长为 3 的回路；v_1 和 v_3 的距离是 2 。

直接观察图8-18，上述结论都可以得到证实。

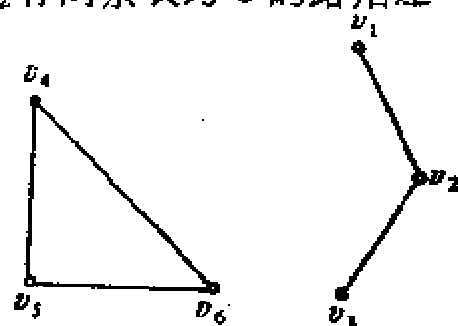


图 8-18

在计算机应用中，除了用邻接矩阵表示图外，还可用关联矩阵、邻接向量矩阵等来表示图。设图G有n个结点$v_1,v_2,\cdots,v_n$，m条边$e_1,e_2,\cdots,e_m$，则G的**关联矩阵**$I=(b_{ij})$是一个$n\times m$矩阵，其中元素

$$b_{ij}=\begin{cases}1 & \text{若 } v_i \text{ 和 } e_j \text{ 是关联的；}\\ 0 & \text{否则。}\end{cases}$$

例如，对图 8-19 所示的图，如果我们将它的边分别标识e_1，$e_2,\cdots,e_7$，则它的关联矩阵

$$I=\begin{array}{c}\\ v_1\\ v_2\\ v_3\\ v_4\\ v_5\end{array}\begin{array}{c}\begin{array}{ccccccc}e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7\end{array}\\ \begin{pmatrix}1 & 1 & 0 & 0 & 0 & 1 & 0\\ 1 & 0 & 1 & 0 & 1 & 0 & 1\\ 0 & 0 & 0 & 1 & 0 & 0 & 1\\ 0 & 0 & 0 & 0 & 1 & 1 & 0\\ 0 & 1 & 1 & 1 & 0 & 0 & 0\end{pmatrix}\end{array}.$$

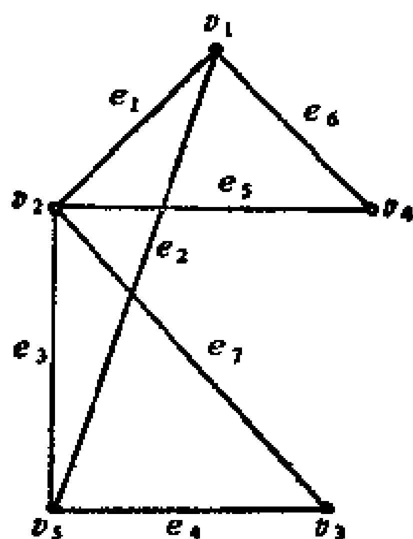


图 8-19

在关联矩阵I中每列都正好包含两个1，并且任何两个列都是不相同的，第i行中1的个数即为结点v_i的次数，在解决各种包含有环的问题时，关联矩阵是有用的，但关联矩阵需要较多的存贮单元。

所谓**邻接向量矩阵**是一个 n 行（$\#V=n$）的矩阵，这 n 行分别与图的 n 个结点对应，第 i 行的元素是与 v_i 邻接的所有结点（$i=1,2,\cdots,n$），我们称这个行向量为**邻接向量**。在这个向量中，元素的次序通常是由边的次序所决定。邻接向量矩阵的列数等于图中各结点的最大次数。

例如，对图 8-19 所示的图，按照图中所标明的边的次序，该图的邻接向量矩阵是：

$$\begin{array}{c} v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{array}\begin{bmatrix} 2 & 5 & 4 & 0 \\ 1 & 5 & 4 & 3 \\ 5 & 2 & 0 & 0 \\ 2 & 1 & 0 & 0 \\ 1 & 2 & 3 & 0 \end{bmatrix}.$$

在对图的边扫视次数不大就可能解决的问题中，邻接向量矩阵是表达图的特别好的工具。

以上各种表示图的方法，其优劣不能一概而论，而取决于所要解决的问题。

对于图 $G=(V,E)$ 中的任意两个结点 v_i 和 v_j，由 G 的邻接矩阵 A 可以确定 G 中是否存在一条连接 v_i 到 v_j 的边；由矩阵 A^l 可以确定 G 中是否存在有连接 v_i 到 v_j 的长为 l 的路以及这样的路的数目。但是，当我们需要知道图 G 是否为连通图时，无论是矩阵 A 还是矩阵 A^l 都无法提供回答。这时，我们可以用下述方法计算出矩阵 B_n（$\#V=n$），即

$$B_n=A+A^2+A^3+\cdots+A^n.$$

矩阵 B_n 的 (i,j) 项元素 b_{ij} 给出连接 v_i 和 v_j 的长度小于或等于 n 的路的总数。如果这个元素不等于零，则结点 v_i 和 v_j 是连接的；如果这个元素等于零，则结点 v_i 和 v_j 不是连接的。若矩阵 B_n 中的每一个元素都不为 0，则图 G 是一连通图；否则图 G 是不连通的图。

矩阵 B_n 的计算显然是相当麻烦的。而且，为了确定G是否为连通图，我们只需知道从 v_i 到 v_j 是否存在有路而并不关心其间路的数目。因此，为了简洁地表达图的连通性，我们定义图G的连接矩阵。

定义 8-9 设图 $G=(V,E)$，其中 $V=\{v_1,v_2,\cdots,v_n\}$，n阶方阵 $C=(c_{ij})$ 称为G的**连接矩阵**，其中元素

$$C_{ij}=\begin{cases}1 & \text{若从 } v_i \text{ 到 } v_j \text{ 存在一条路；}\\ 0 & \text{否则。}\end{cases}$$

显然，当且仅当矩阵 $C=(c_{ij})$ 的所有元素均为1时，图G是连通的。

由矩阵 B_n 可以确定连接矩阵C，但正如前面所说，矩阵 B_n 的计算过于复杂。下面我们给出由邻接矩阵A求连接矩阵C的一种较为简单的方法。

如果一个矩阵的所有元素均为0或1，则这种矩阵称为是**布尔矩阵**。对于布尔矩阵来说，若矩阵运算中元素的相加与相乘均规定为布尔加与布尔乘（参见 §2.4），则这种矩阵运算称为是**布尔矩阵运算**。在布尔矩阵运算下，我们用 $A^{(i)}$ 表示矩阵A的i次幂，用[+]和[·]表示矩阵的相加与相乘。

根据布尔矩阵运算的定义，对于邻接矩阵A，矩阵$A^{(2)}$的(i,j)项元素 $a_{ij}^{(2)}=\sum_{k=1}^{n}a_{ik}a_{kj}$，其中的加与乘都是布尔型的。因此，当且仅当存在某个$k(1\leqslant k\leqslant n)$使得 $a_{ik}=1$ 且 $a_{kj}=1$ 时，有 $a_{ij}^{(2)}=1$。此即当且仅当存在有连接 v_i 到 v_j 的长为2的路时，$A^{(2)}$的(i,j)元素 $a_{ij}^{(2)}=1$。类似地，对于任意的正整数l，当且仅当存在有连接 v_i 到 v_j 的长为l的路时，$A^{(l)}$的(i,j)项元素 $a_{ij}^{(l)}=1$。由此可知，连接矩阵可以按下述方法求得：

$$C=A[+]A^{(2)}[+]\cdots[+]A^{(n)}.$$

例如，由图 8-18 的邻接矩阵A可求得

$$A^{(2)}=\begin{pmatrix}1&0&1&0&0&0\\0&1&0&0&0&0\\1&0&1&0&0&0\\0&0&0&1&1&1\\0&0&0&1&1&1\\0&0&0&1&1&1\end{pmatrix},\quad A^{(3)}=\begin{pmatrix}0&1&0&0&0&0\\1&0&1&0&0&0\\0&1&0&0&0&0\\0&0&0&1&1&1\\0&0&0&1&1&1\\0&0&0&1&1&1\end{pmatrix},$$

$$A^{(4)}=\begin{pmatrix}1&0&1&0&0&0\\0&1&0&0&0&0\\1&0&1&0&0&0\\0&0&0&1&1&1\\0&0&0&1&1&1\\0&0&0&1&1&1\end{pmatrix},\quad A^{(5)}=\begin{pmatrix}0&1&0&0&0&0\\1&0&1&0&0&0\\0&1&0&0&0&0\\0&0&0&1&1&1\\0&0&0&1&1&1\\0&0&0&1&1&1\end{pmatrix},$$

$$A^{(6)}=\begin{pmatrix}1&0&1&0&0&0\\0&1&0&0&0&0\\1&0&1&0&0&0\\0&0&0&1&1&1\\0&0&0&1&1&1\\0&0&0&1&1&1\end{pmatrix}.$$

因而 $C=A[+]A^{(2)}[+]\cdots[+]A^{(6)}=\begin{pmatrix}1&1&1&0&0&0\\1&1&1&0&0&0\\1&1&1&0&0&0\\0&0&0&1&1&1\\0&0&0&1&1&1\\0&0&0&1&1&1\end{pmatrix}$.

由于矩阵中存在有为 0 的元素，因此图 8-18 不是连通的。直接观察图 8-18 也可得到同样的结论。

§8.3 欧拉图和哈密顿图

在图的应用中出现的一个共同问题是：给定一个图G，是否能找到一个回路，它通过G的每条边一次且仅一次？这样的回路称为**欧拉回路**。具有欧拉回路的图称为**欧拉图**。

欧拉图的概念是欧拉（Leonhard Euler，瑞士数学家，1707-1783）在1736年引入的，他用一条非常简单的准则解决了哥尼斯堡(Königsberg)七桥问题。哥尼斯堡城位于普雷格尔(Pregel)河的两岸及河中的两个岛屿上，该城市的各部分由图8-20(a)所示的七座桥相连接，当时城中的居民热衷于这样一个问题：游人从四块陆地区域中的任何一块出发，怎样走才能做到恰好通过每座桥一次而返回到原来的出发区域。问题看起来很简单，但当时谁也解决不了。为了解决这个问题，欧拉将每一块陆地区域用一个结点表示，每一座桥用连接相应两个结点的一条边来表示，于是得到一个多重图，如图8-20(b)所示。因此，哥尼斯堡七桥问题就变为：在这个多重图中是否存在一条欧拉回路？欧拉证明了

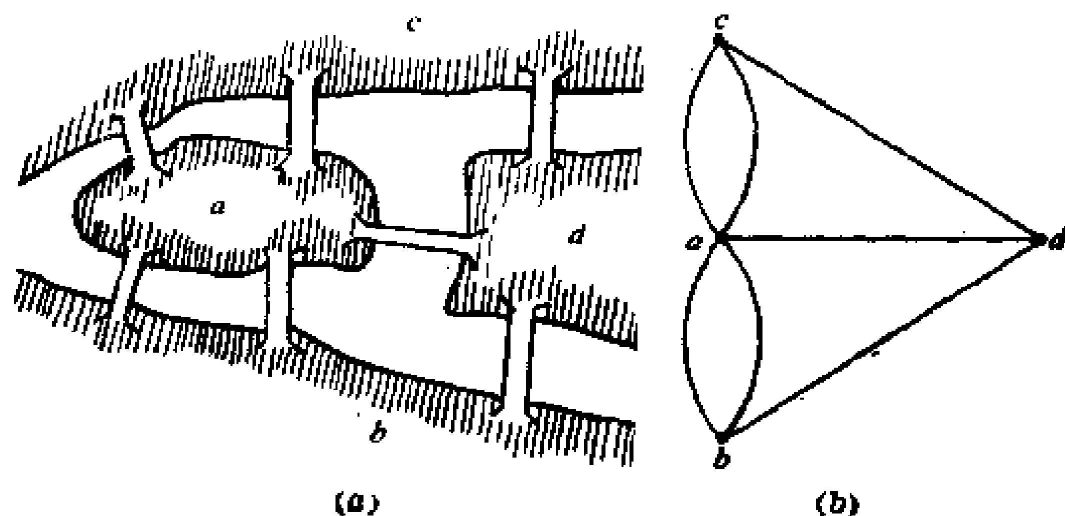


图 8-20

下面的定理，从而对哥尼斯堡七桥问题给予了否定的回答，即图8-20(a)中的七座桥不能按上述的要求走遍。

显然，除了有孤立点的情形外，一个欧拉图是一个连通图。图8-2是欧拉图的一个例子，它的一个欧拉回路是$v_1v_2v_3v_4v_5v_2v_4v_1v_3v_5v_1$。而图8-1不是欧拉图，这可由欧拉给出下述定理来证实。

定理8-3 一个连通图G为欧拉图的充要条件是G的每一结点具有偶次数。

证明 设G是一欧拉图，并设α是G中的一个欧拉回路。每当α通过G的一个结点时，α通过关联于这个结点的两条边，并且这两条边是α以前未走过的，因此，若α通过某一结点k次，则通过关联于该结点的$2k$条边。由于在α中G的每条边出现一次且仅一次，因此每个结点的次数必是2的倍数。

反之，设图G的每个结点具有偶次数，要证明图G是一欧拉图，我们用对图G的边数m进行归纳的方法来证明。

当$m=0$时，图G是平凡图。我们认为它是一个欧拉图，因此结论成立。

当$m=3$时，结论显然成立(注：$m=1$和$m=2$时，图中每个结点不可能具有偶次数)。

设对于$k=3,4,\cdots,m$，任何具有k条边的连通图结论均成立，并设图G是一具有$m+1$条边且每个结点具有偶次数的连通图。从图G的任一结点a出发沿任一边前进，但决不在任一边上行走两次，便可确定一条路。当到达任一结点$v\neq a$时，因它只使用过v的奇数条边，它将仍能沿着某一边前进，当它无法再前进时，它必是到达了a。因此构成一回路α。如果图G的所有边全被使用完，则α便是一欧拉回路。若所有的边没有被使用完，令剩下的图为G'(由除去α后剩下的边及剩下的边所关联的结点所组成)，设$H_1,H_2,\cdots,H_k$是G'的k个分图，因为G'的所有结点

都仍是偶次数，所以 H_i 的边数不为 1 和 2 ($i=1,2,\cdots,k$)，根据归纳假设，这些部分各有欧拉回路，设为 $\mu_1,\mu_2,\cdots,\mu_k$，因图 G 是连通的，路 α 必与所有的 $H_i(i=1,2,\cdots,k)$ 有公共结点，分别令其为 $v_1,v_2,\cdots,v_k$，则回路

$$\alpha[a,v_1]+\mu_1+\alpha[v_1,v_2]+\mu_2+\cdots+\alpha[v_{k-1},v_k]+\mu_k+\alpha[v_k,a]$$

就是一条欧拉回路。定理证完。

例如，图8-21是一欧拉图，因为它的每一个结点具有偶次数。从结点 a 出发，沿边 $\{a,v_1\}$ 前进可得一回路 $\alpha=av_1v_4v_5a$。剩下的图 G' 有两个分图，分别有欧拉回路 $\mu_1=v_1v_2v_3v_1$，$\mu_2=v_5v_6v_7v_5$。v_1 是 α 与 μ_1 的公共结点，v_5 是 α 与 μ_2 的公共结点。由此，该图的一个欧拉回路为

$$av_1v_2v_3v_1v_4v_5v_6v_7v_5a.$$

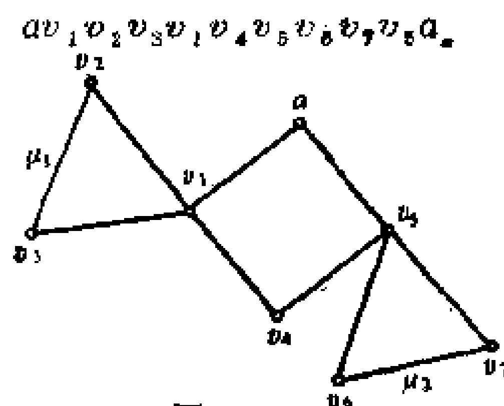


图 8-21

用同样的方法可以证明，定理 8-3 对于多重图也是成立的。在哥尼斯堡桥的问题中，由于图 8-20(b) 所示的多重图中没有任何结点是偶次数，故答案是否定的。

通过图 G 的每条边一次且仅一次的开路称为图 G 的**欧拉路**。

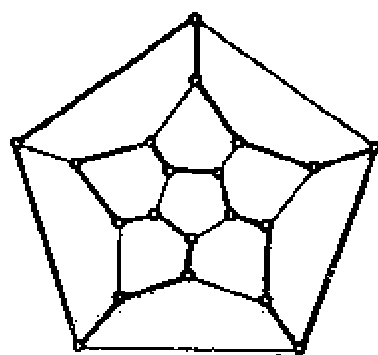
定理 8-4 连通图 G 具有一条连接结点 v_i 和 v_j 的欧拉路的充要条件是 v_i 和 v_j 是 G 中仅有的具有奇次数的结点。

证明 将边 $\{v_i,v_j\}$ 加于图 G 上，令其所得的图为 G' (G' 可能为多重图)，那么当且仅当 G' 有一欧拉回路时，G 有连接 v_i 到 v_j 的一欧拉路。即当且仅当 G' 的所有结点均为偶次数时，也就

是当且仅当G的所有结点除 v_i 和 v_j 是奇次数外均为偶次数时，G有一连接 v_i 到 v_j 的欧拉路。定理得证。

在图的理论和应用中出现的另一个共同问题是：给定一个图G，是否能找到一个环，它通过图G的每个结点一次且仅一次？这样的环称为**哈密顿**（William Hamilton，爱尔兰数学家，1805-1865）**环**。具有哈密顿环的图称为**哈密顿图**。类似地，我们定义**哈密顿路**是通过图G的每个结点一次且仅一次的开路。显然，每个哈密顿图都一定是连通的。图 8-1、8-2、8-4 和 8-5 都是哈密顿图，其中的哈密顿环是显而易见的。

虽然确定哈密顿环（或路）的存在性问题与确定欧拉回路（或路）的存在性问题同样地有意义，但至今为止，还没有发现一个简单的必要充分条件，我们只好通过具体构造这样一个环（或路）来指出一个给定图有一条哈密顿环（或路）。例如，图8-22中粗线的边构成一条哈密顿环。


图 8-22

类似于确定哈密顿环的一个问题是流动售货员的问题。设有一个流动售货员要从公司出发走销附近所有的城镇，然后返回公司所在地，那么他将如何安排他的路线，使得旅行的总距离最小？该问题用图解法来表示，可用结点代表公司所在地及各城镇，用边代表相互之间的公路，并标出相应公路之长度（假定每两个城镇之间都有公路），这样，该问题就简化为在一个完全图上找出一条经过每个结点一次且仅一次而且全程为最短的环来。同样，对此问题也没有完美的解决方法。下面给出一个“最邻近方法”，它为解决此问题给出了一个较好的结果。

1. 由任意选择的结点开始，找一个与起始结点最近的结点，形成一条边的初始路径。

2. 设 x 表示最新加到这条路上的结点，从不在路上的所有结点中间选一个与 x 最接近的结点，将连接 x 与这一结点的边加到这条路上。

重复这一步，直到 G 中所有结点包含在路上。

3. 将连接起始点与最后加入的结点之间的边加到这条路上，就得到一个环。

例如，对于图 8-23(a) 所示的图，我们从结点 v_1 开始，根据最邻近方法一步一步地构造一个哈密顿环，其过程如图 8-23(b) 到 8-23(e) 所示。这一条环的总距离是40。图 8-23(f) 给出了最小哈密顿环的总距离是37。

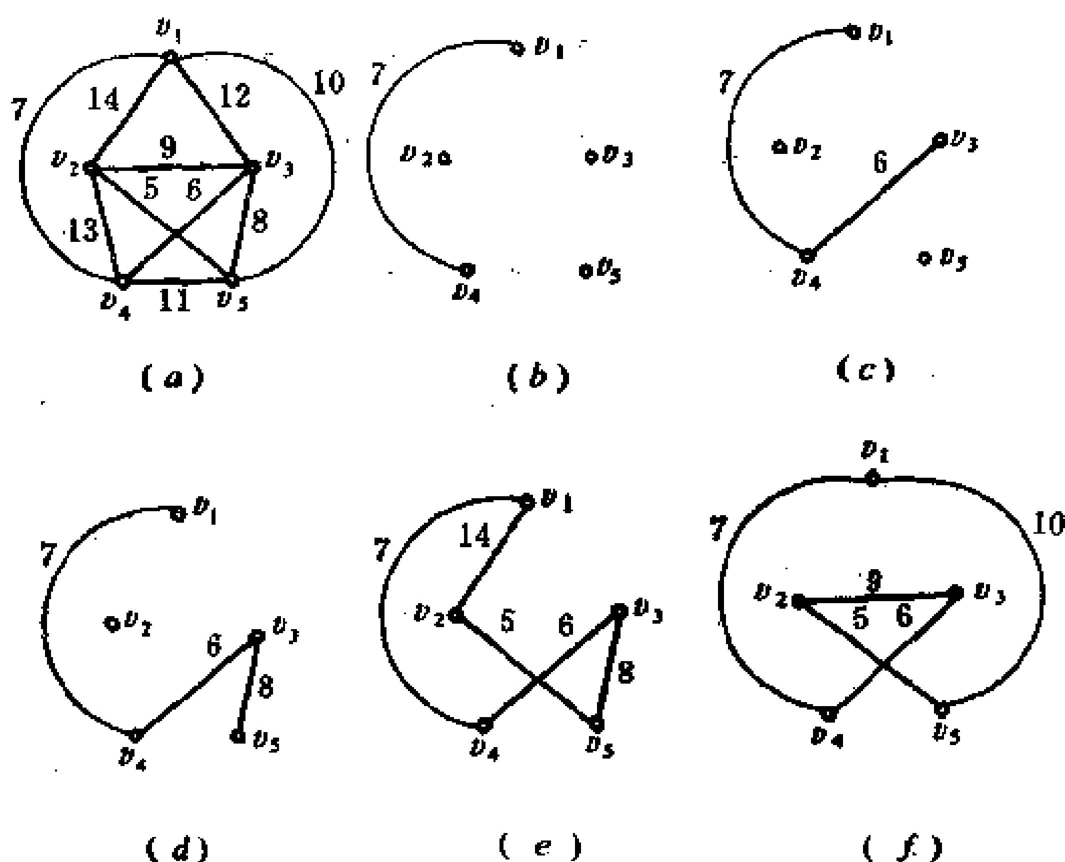


图 8-23

§8.4 树

在各种各样的图中，有一类特别重要也比较简单的图，称为树。

定义 8-10 不包含环的连通图称为**树**。不包含环的图（即每个分图都是树的图）称为**树林**。

图8-24给出了四棵树。

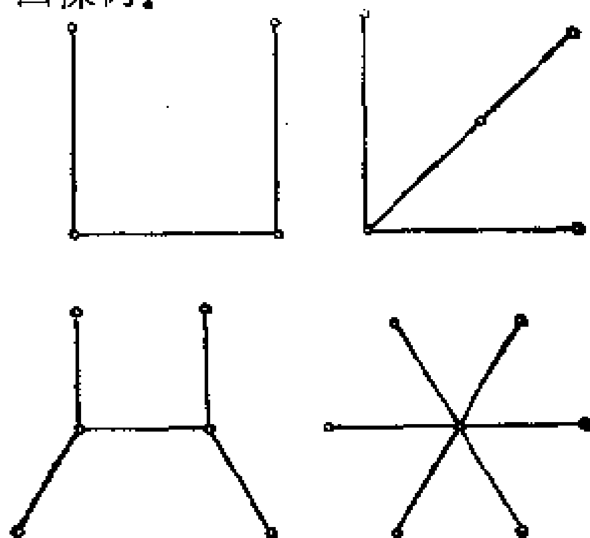


图 8-24

若把图8-24中的四棵树看作是一个图G的四棵树，则G就是一个树林。

每一棵树都至少有一个结点。一个孤立结点也是一棵树。

下面介绍树的一些性质。

定理 8-5 设T是一棵树，v_i和v_j是T中任意两个不同的结点，则v_i和v_j由唯一的一条真路相连接。若v_i和v_j不相邻接，那末，当给T添加一条边$\{v_i, v_j\}$后形成的图恰有一个环。

证明 由于T是连通的，因此必存在一路从而必存在一真路连结v_i和v_j。

设$\alpha = v_i a_1 a_2 \cdots a_r v_j$和$\beta = v_i b_1 b_2 \cdots b_s v_j$是连接$v_i$和$v_j$的两

条不同的真路，记 $v_j=a_{r+j}=b_{s+1}$， 设 k 是使得 $a_k \neq b_k$ 的最小正整数。因为 α 和 β 不同，这样的 k 必存在。又因为 $a_{r+1}=b_{s+1}$，所以有 $h_1, h_2 \geqslant k$，使得 $a_{h_1}=b_{h_2}$，且 $a_k, a_{k+1}, \cdots, a_{h_1-1}$ 不在 β 上，$b_k, b_{k+1}, \cdots, b_{h_2-1}$ 不在 α 上，于是 α 在 a_{k-1} 与 a_{h_1} 之间的一段子路和 β 在 b_{k-1} 与 b_{h_2} 之间的一段子路合起来构成一个环，与 G 是一个树矛盾，从而 T 中连接 v_i 和 v_j 的真路是唯一的。

若 v_i 和 v_j 不相邻接，则将边 $\{v_i, v_j\}$ 添加于 T 后，连接 v_i 和 v_j 的唯一的真路 α 和边 $\{v_i, v_j\}$ 一起在新图中形成一环，因为 T 中不存在除 α 以外连接 v_i 和 v_j 的其他真路，因此边 $\{v_i, v_j\}$ 不能和其他任一真路形成环。定理得证。

定理 8-6 在 (n, m) 树中，$m=n-1$。

证明 （对结点数 n 进行归纳）

当 $n=1$ 和 $n=2$ 时，定理显然成立。

设对结点数少于 n 的所有树定理成立，而 T 是一 (n, m) 树，由于 T 不包含任何环，因此从 T 中移去任何一条边都将把 T 变成一具有两个分图的图。这两个分图也必然是树，设它们分别是 (n_1, m_1) 树和 (n_2, m_2) 树，由归纳假设 $m_1=n_1-1$，$m_2=n_2-1$，又因为 $n=n_1+n_2$，$m=m_1+m_2+1$，所以有 $m=n-1$。因此定理成立。

若 G 是由 r 棵树构成的一 (n, m) 树林，则定理 8-6 很容易推广而得到关系式 $m=n-r$。

如果我们把树中次数为 1 的结点称为**树叶**，则有下面的定理.

定理 8-7 具有两个或更多结点的树至少有两片树叶。

证明 设 T 是一 (n, m) 树，其中 $n \geqslant 2$。显然，T 中所有结点的次数之和 $S=2m$。又由定理 8-6，$S=2n-2$。假设 T 中树叶少于两片，则 T 中至少有 $n-1$ 个结点的次数不小于 2，故 T 中所有结点的次数之和 $S>2n-2$，这与 $S=2n-2$ 相矛盾，因此 T 至少有两片树叶。证完。

树的有些特征可用来作为树的定义，我们列出下面三条，要证明这些定义与定义8-10的等价性并不困难，留给读者自己作为练习。

1. 每两个结点之间由唯一的真路相连接的图是树。

2. $m=n-1$ 的连通图是树。

3. $m=n-1$ 且无环的图是树。

若连通图G的一个生成子图T是一棵树，则称T为G的**生成树**。显然，任何连通图都有生成树。而且一般来说，它的生成树不是唯一的。例如图 8-25(*b*) 和(*c*)都是图 8-25(*a*) 的生成树。

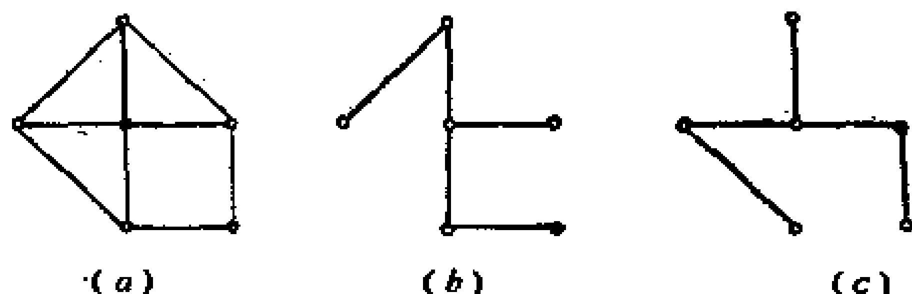


图 8-25

由生成树的定义我们可以看出，一个图G与它的生成树的差别在于前者可能包含有环，而后者不包含任何环。因此，我们可以用去掉图G中的环而不破坏图G的连通性的方法由图G构造出它的生成树。

算法 8-1

给出连通图G，构造其生成树T_G：

(1) 令 G 为G_1。置 i 为 1；

(2) 若 G_i 无环，则 $T_G=G_i$；否则

(3) 在 G_i 中找出任一环 σ_i，并从 σ_i 中删去任一边 e_i，称这剩余的图为 G_{i+1}，由于e_i是 G_i 的一个环中的边，所以 G_{i+1} 包括了G_i的所有结点，并且若G_i是连通的，则G_{i+1}也同样是连通的，

(4) i 增加 1，并返回到第(2)步。

在上述重复过程中，每一次都有G的一个环被“弄破”。由于G中环的个数是有限的，因此对某个i，我们最后能得到一个图G_i，它包含G的所有结点但不包含环，于是根据定义，G_i就是T_G。当然，由此算法得到的T_G不是唯一的，因为在算法的每一次反复中，σ_i和e_i都不一定是唯一的。

若G是一(n, m)连通图，则由定理8-6，T_G是一$(n, n-1)$图，因此，在得到T_G前必须删去的边的总数必然为$m-(n-1)$。该数称为G的**环秩**。因此，G的环秩是为了“弄破”G的所有环而必须由G中删去的边的最小数目。这些被删去的每一条边称为是相应生成树T_G的**弦**，而在生成树T_G中的边称为是T_G的**枝**。

图8-26以一(6, 9)连通图G说明了算法8-1。在此例中，T_G有$6-1=5$条边，而G的环秩为$9-5=4$。

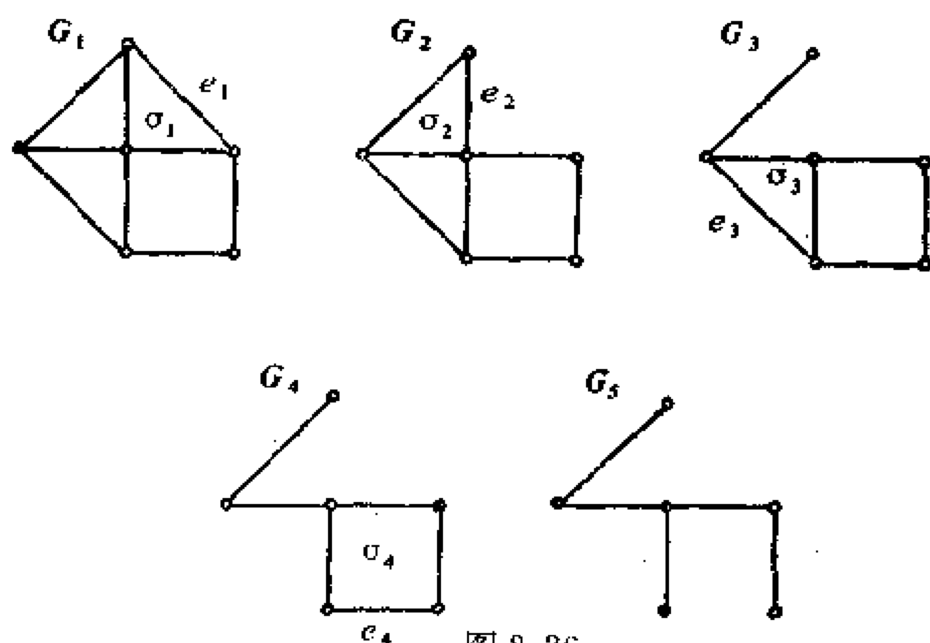


图 8-26

现在我们考虑一个更普遍的问题，即如何决定每条边都以实数值赋权的有权图的最小生成树问题。设$G=(V, E, f)$是一连通的有权图，若T是G的一棵生成树，T的树枝的集合为$E(T)$，则T的所有树枝的权的和$W(T)=\sum_{e\in E(T)} f(e)$称为$T$的权。若生成

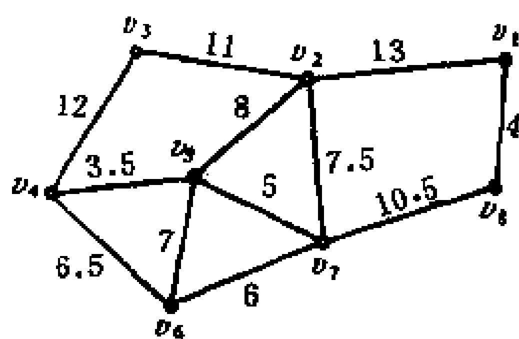
树T_0在所有生成树中有最小的权，则称T_0是G的**最小生成树**。这个问题也具有明显的实际背景，例如设图G中的结点表示一些城市，边表示城市之间的公路，边的权表示公路的长度。如果我们要用通讯线路把这些城市联系起来，并且线路要求沿着道路架设，如何使得所用的线路最短呢？这个问题实质上就是求G的最小生成树的问题。其他如水渠的布置，交通线的规划等等都与这个问题有关。

下面介绍一种求最小生成树的算法。

算法 8-2 （克鲁斯克尔（Kruskal）算法）

设$G=(V,E,f)$是一具有n个结点的连通有权图，构造G的最小生成树：

(1) 选取G中一条边e_1，使e_1在G的所有边中有最小的权。令$G_1=(V,S_1)$，$S_1=\{e_1\}$。置i为1；



(a)

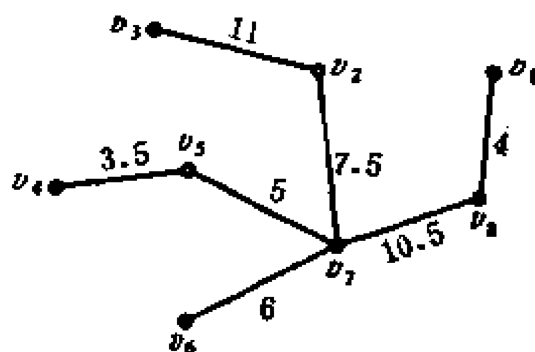
(2) 若已选好$S_i=\{e_1,e_2,\cdots,e_i\}$，从$E-S_i$中选一条边$e_{i+1}$使其满足下列条件：

(i) $S_i\cup\{e_{i+1}\}$中不含有环；

(ii) 在$E-S_i$的满足(i)的所有边中，e_{i+1}有最小的权。

若满足上述条件的边e_{i+1}不存在，则$G_i=(V,S_i)$就是最小生成树。否则令$S_{i+1}=S_i\cup\{e_{i+1}\}$，$G_{i+1}=(V,S_{i+1})$；

(3) i增加1，并返回到第(2)步。



(b)

图 8-27

例如在图 8-27(a)所给出的图G中，我们逐次取边v_4v_5，v_1v_8，

v_6v_7，v_8v_7，v_2v_7，v_7v_8，v_2v_3，构成如图 8-27(b) 所示的最小生成树。

定理 8-8 算法8-2给出的 $G_r=(V, S_r=\{e_1, e_2, \cdots, e_r\})$ 是G的最小生成树。

证明 由算法停止的条件可知，G_r 是G的一棵生成树，设 $T_0=(V, E(T_0))$ 是G的一棵最小生成树，我们将证明G_r和T_0具有相同的权。

因为G的结点数为n，所以 G_r与T_0都有 $n-1$条边。若 $S_r=E(T_0)$，则G_r显然就是最小生成树；若 $S_r \neq E(T_0)$，则必存在一条边 $e_i \in S_r$，使得 $e_i \notin E(T_0)$，但 $e_1, e_2, \cdots, e_{i-1}$ 都在 $E(T_0)$ 中，将 e_i 添加到T_0中，由定理8-5，必产生一个唯一的环 C。因为G_r是树，所以环C中至少存在一条边 e' 不在 S_r 中，在树T_0中添加 e_i 而删去 e'，令得到的新树为 T'，则

$$W(T')=W(T)+f(e_i)-f(e'),$$

因为 T_0 是最小生成树，所以有 $W(T') \geqslant W(T_0)$，因而 $f(e_i)-f(e') \geqslant 0$，即 $f(e_i) \geqslant f(e')$，由于 $e_1, e_2, \cdots, e_{i-1}$ 都在 $E(T_0)$ 中，它们与 e' 不构成环，因此，若是 $f(e_i)>f(e')$，则与 e_i 的选取方法矛盾，于是 $f(e_i)=f(e')$，故 T' 也是一棵最小生成树。

反复使用上述的转换，树 T_0 可以转换成 G_r 而权没有任何增加，故 G_r 是一棵最小生成树。证完。

§8.5 有向树

无向图中许多概念和性质，只要略加修改都可以推广到有向图。关于这些，我们在§8.8中将详细介绍。本节我们先介绍有向树的概念。

首先，类似于无向图可以定义有向图中的路。有向图G中 l 条边的序列 (v_{i_0}, v_{i_1})，(v_{i_1}, v_{i_2})，(v_{i_2}, v_{i_3})，$\cdots$，$(v_{i_{l-1}}, v_{i_l})$ 称为连

接 v_{i_0} 到 v_{i_l} 的长度为 l 的**有向路**（或简称为从 v_{i_0} 到 v_{i_l} 的路）。它可表示为 $(v_{i_0},v_{i_1})(v_{i_1},v_{i_2})\cdots(v_{i_{l-1}},v_{i_l})$ 或简单地表示为 $v_{i_0}v_{i_1}\cdots v_{i_{l-1}}v_{i_l}$。若在无向图的开路、回路、真路和环的定义中，将"路"改为"有向路"，我们就得到相应于有向图的这些术语的定义。

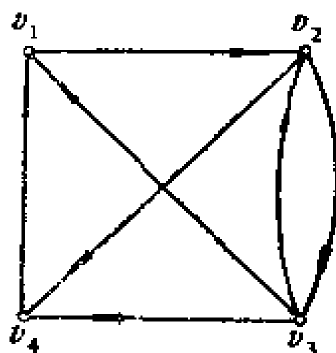


图 8-28

例如在图8-28所显示的有向图中，$v_1v_2v_3v_4$ 是一条从 v_1 到 v_4 的长为 3 的开路，也是一条真路。$v_2v_4v_1v_2v_3$ 和 $v_1v_2v_3v_1v_2v_4$ 是开路，但都不是真路。$v_1v_2v_3v_2v_4v_1$ 是一条长为 5 的回路，但不是环。$v_1v_2v_3v_4v_1$ 是一个环。

在有向图中，结点 v_i 和 v_j 分别称为边 (v_i,v_j) 的**始点**和**终点**。对于任何结点 v，以 v 为始点的边的条数称为结点 v 的**引出次数**，以 v 为终点的边的条数称为结点 v 的**引入次数**。v 的引入次数和引出次数之和称为结点 v 的**次数**，并记作 $\deg(v)$。例如图 8-28 中结点 v_3 的引出次数是 3，引入次数是 1。结点 v_1 的引出次数是 1，引入次数是 2。

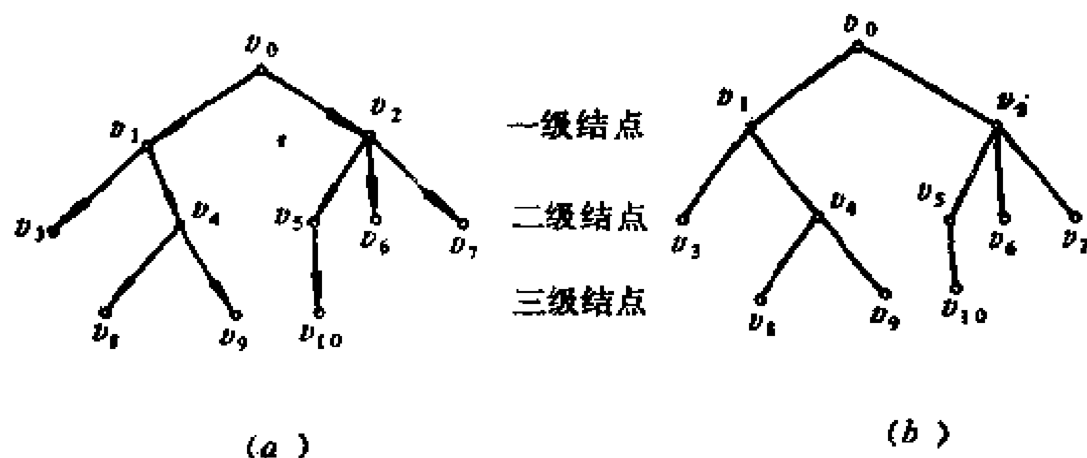
定义 8-11 一个不包含环的有向图 G，若它只有一个结点 v_0 的引入次数是 0，而所有其他结点的引入次数都等于 1，则称 G 为**有向树**。结点 v_0 称为树的**根**。

每一棵有向树至少有一个结点。一个孤立点也是一棵有向树。

在有向树中引出次数为 0 的结点称为**终点**或**树叶**，不是树叶

的所有其它结点称为**分枝结点**. 不难证明，在有向树中对任一结点 $v_i \in V$，必存在唯一的一条从根 v_0 到 v_i 的真路，我们称从 v_0 到结点 v_i 的距离为结点 v_i 的**级**。当然，根的级是 0。

当用图解法表示有向树时，由于根 v_0 的引入次数为 0，因此，没有边进入 v_0，与 v_0 相关联的边都是从 v_0 发出的，这些从 v_0 发出的边分别进入到 1 级结点，由于 1 级结点的引入次数是 1，故它们不可能再从其他结点进入新的边。因此，若还有边与 1 级结点相关联，必是从这些 1 级结点发出的。1 级结点发出的边分别进入到 2 级结点. 如此下去，可得有向树必为图 8-29(*a*) 所示的样子。



(*a*)　　　　(*b*)

图 8-29

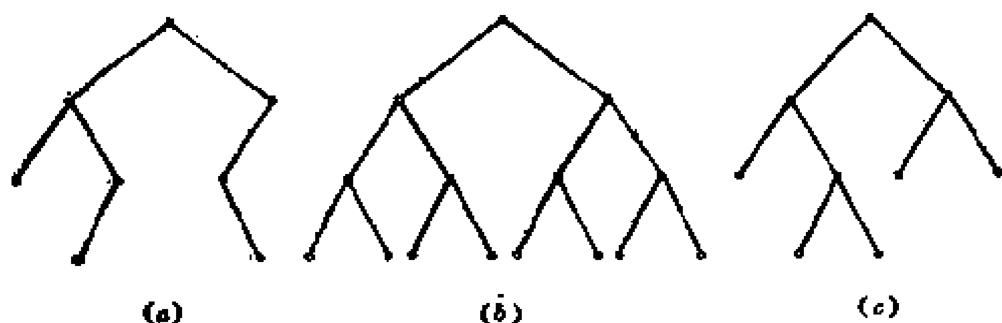
我们方便地把树的根画在图的上部，叶画在下部. 这是文献中普遍使用的方法，而不用树的自然生长表示法. 由于所有的箭头都是朝下的，因此我们常省略边的箭头. 例如，图 8-29(*a*) 可用图 8-29(*b*) 所示的方式来表示。

在一有向树中，如果从 v_i 到 v_j 有一条边，则称结点 v_j 是 v_i 的儿子，或称 v_i 是 v_j 的父亲。若结点 v_j 和 v_k 是同一结点的儿子，则称 v_j 和 v_k 是兄弟. 若从 v_i 到 v_j 有一条有向路， 则称结点 v_j 是结点 v_i 的子孙，或称 v_i 是 v_j 的祖先。这说明通常的家族关系可以用一棵有向树来表示。

在有向树T中，由结点v和它的所有子孙所构成的结点子集$V'\subseteq V$以及从v出发的所有有向路中的边所构成的边集E'组成T的子图$T'=(V',E')$，称为是以v为根的**子树**．v的子树是以v的儿子为根的子树．例如，图8-29(a)中v_0有两棵子树，它们的结点集分别是$\{v_1, v_3, v_4, v_8, v_9\}$和$\{v_2, v_5, v_6, v_7, v_{10}\}$．这两棵子树的根分别是$v_1$和$v_2$．结点$v_2$有三棵子树，它们的根分别是$v_5, v_6, v_7$．

定义 8-12 在一有向树中，若每一个结点的引出次数都小于或等于m，则称这树为**m元树**．若每一个结点的引出次数都等于m或0，则称这树为**完全m元树**．

特别，当$m=2$时，就得到**二元树**和**完全二元树**．二元树的每个结点v至多有两棵子树，分别称为v的**左子树**和**右子树**．若v仅有一棵子树，则可称它为v的左子树或右子树．在图解中，左子树画在v的左下方，右子树画在v的右下方．图8-30给出了三棵二元树．其中(b)和(c)是完全二元树．



(a) (b) (c)

图 8-30

在计算机科学中有着广泛应用的是二元树．我们可以用二元树唯一地表示每一棵树．这样，对于树的计算机表示，只要考察相应的二元树的表示就可以了．下面我们介绍用二元树T'来表示任一有向树T，且保持T中每一结点的子树的有序性的一种方法：设T中结点v_i的r棵子树有根$v_{i_1}, v_{i_2}, \cdots, v_{i_r}$，其顺序自左向右，则在$T'$中$v_{i_1}$是$v_i$的左儿子，$v_{i_2}$是$v_{i_1}$的右儿子，$v_{i_3}$是$v_{i_2}$

的右儿子，…，v_{i_k} 是 $v_{i_{k-1}}$ 的右儿子．例如，图 8-31 给出了这种方法的一个实例．

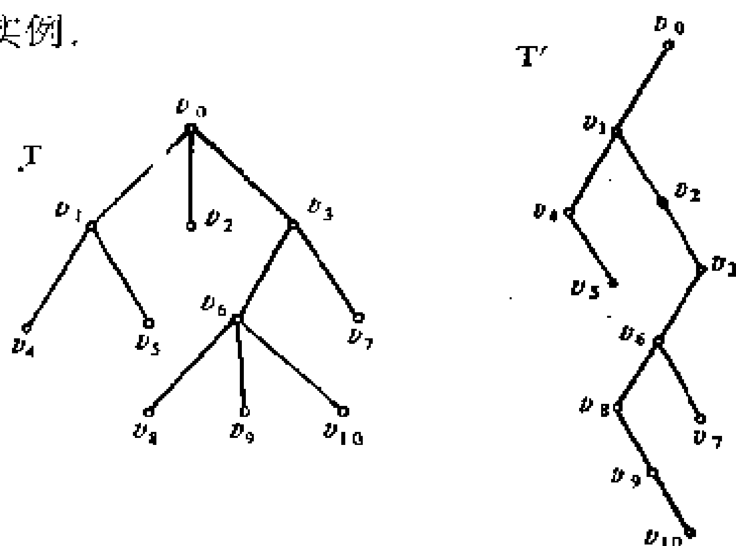


图 8-31

可看出 T' 中构成子树“左边界”的路（如 $v_0v_1v_4$ 或 $v_3v_6v_8$）是 T 中一相似的边界．T' 中构成子树的“右边界”的路（如 $v_1v_2v_3$ 或 $v_8v_9v_{10}$）是 T 中同一结点的儿子集（如 v_1，v_2 和 v_3 都是 v_0 的儿子）．于是由 T 的二元表示 T' 重新构造其原树 T 就只是一件简单的事情了．

在计算机应用中常出现的一个问题是：如何有顺序地通过一棵二元树，使得每一结点恰好被访问一次．下面给出实现这一任务的几种最常用的算法（所有算法均是递归地描述）．

1．先根通过：

（1）访问根．（2）在根的左子树上执行先根通过．（3）在根的右子树上执行先根通过．

2．中根通过：

（1）在根的左子树上执行中根通过．（2）访问根．（3）在根的右子树上执行中根通过．

3．后根通过：

（1）在根的左子树上执行后根通过．（2）在根的右子树上执行后根通过．（3）访问根．

例如，运用这三种方法通过图8-32所示之树的结点的顺序分别如下

先根：$v_0v_1v_3v_4v_6v_2v_5v_7v_8v_9$；

中根：$v_3v_1v_6v_4v_0v_5v_8v_7v_9v_2$；

后根：$v_3v_6v_4v_1v_8v_9v_7v_5v_2v_0$。

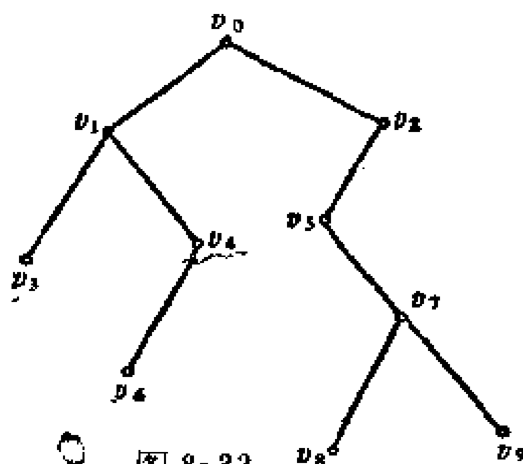


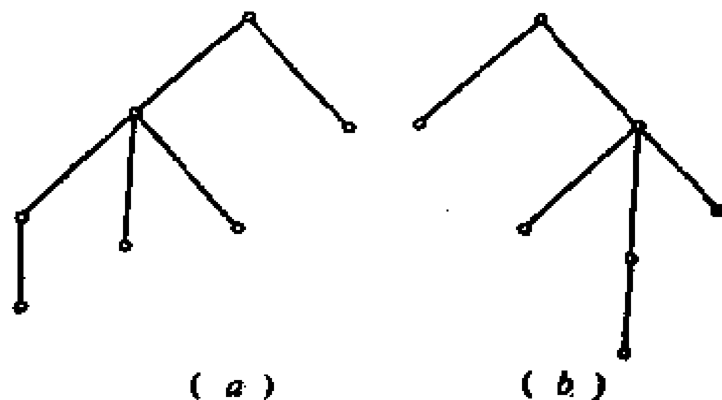
图 8-32

在上面所讨论的有向树中，我们没有考虑同一级结点的次序。例如在图 8-33 中，(*a*) 和 (*b*) 被认为是表示同一棵有向树。但在许多具体问题中，往往需要考虑同一级上结点的次序。

定义 8-13 在有向树中，若规定了每一级上结点的次序，则这样的有向树称为**有序树**。

一般地，在画出的有序树中，规定同一级结点的次序为从左到右。

例如，图 8-33(*a*) 和 (*b*) 是两棵不同的有序树。



(*a*) (*b*)

图 8-33

从图 8-34 可以看到一个句子的结构如何用一棵有序树来表示。

作为另一个例子，我们可以看到一个算术表达式怎样表示成一棵有序树。例如，算术表达式 $(((a+b*c)*d-e)/(f+g))+h*i*j$ 能表示成图 8-35。在这里，被操作数出现在树叶的位置上，操作符出现在分枝点的位置上。当用一棵二元树来表示一个算术表达式时，就不再需要括号。

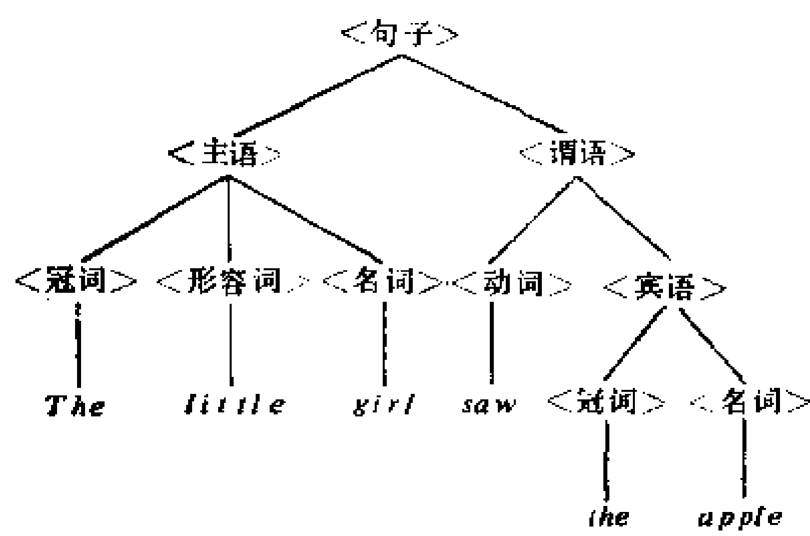


图 8-34

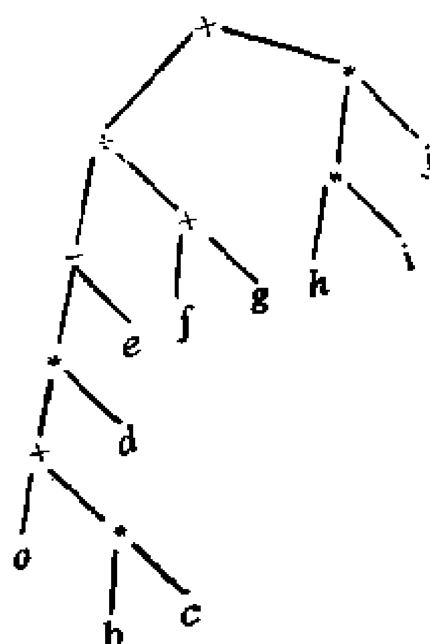


图 8-35

§8.6 偶 图

本节讨论另外一种特殊类型的图。

定义 8-14 若一个图 G 的结点集 V 能分为两个子集 V_1 和 V_2，以使 G 的每一条边具有形式 $\{v_i, v_j\}$，其中 $v_i \in V_1$，$v_j \in V_2$，即 G 的每一条边将连接 V_1 中的某结点到 V_2 中的某结点，则这样的图 G 称为是一个**偶图**。子集 V_1 和 V_2 称为 G 的**互补结点子集**。

图8-36给出了一个具有7个结点的偶图，它的互补结点子集是$V_1=\{v_1,v_2,v_3,v_4\}$和$V_2=\{v_5,v_6,v_7\}$。

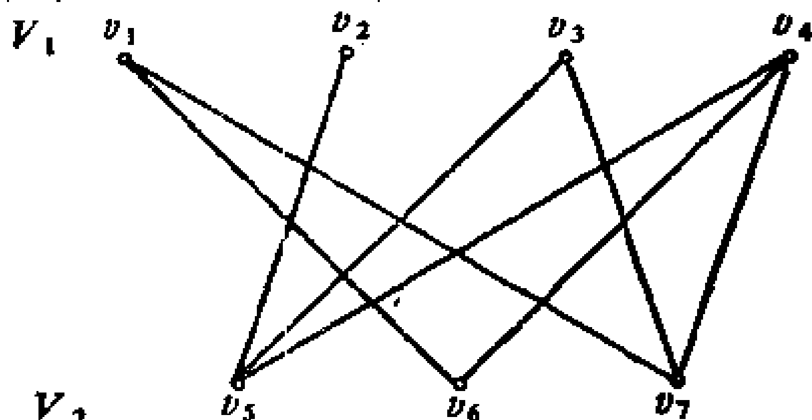


图 8-36

定理 8-9 图G为偶图的充要条件是它的所有回路均为偶数长。

证明 设G是一个偶图，则它的结点集V能分为两个子集V_1和V_2，并且若$\{v_i,v_j\}$为其边，则$v_i\in V_1$，$v_j\in V_2$。令$v_{i_0}v_{i_1}v_{i_2}\cdots v_{i_{l-1}}v_{i_0}$为$G$中任一长度为$l$的回路。不失一般性，设$v_{i_0}\in V_1$，于是$v_{i_0},v_{i_2},v_{i_4},\cdots\in V_1$，$v_{i_1},v_{i_3},v_{i_5},\cdots\in V_2$，因而$l-1$为奇数，即$l$必为偶数。

反之，设G中每一回路的长度均为偶数，并设G是连通的。定义V的子集$V_1=\{v_i|v_i$和某一固定结点v之间的距离为偶数$\}$，$V_2=V-V_1$。

假设有一条边$\{v_i,v_j\}$存在，其$v_i,v_j\in V_1$，则由v和v_i间的短程(偶数长)，边$\{v_i,v_j\}$及v_j和v之间的短程(偶数长)所组成的回路必具有奇数长。得出矛盾。因此G中无边具有形式$\{v_i,v_j\}$，而$v_i,v_j\in V_1$。其次，假设有一条边$\{v_i,v_j\}$存在，其$v_i,v_j\in V_2$，则由v和v_i间的短程(奇数长)，边$\{v_i,v_j\}$及v_j和v间的短程(奇数长)所组成的回路必具有奇数长。又得出矛盾。于是G中的每一条边必具有形式$\{v_i,v_j\}$，其中$v_i\in V_1$，$v_j\in V_2$，即G是具有互补结点子集V_1和V_2的一偶图。

若G中每一回路的长为偶数，但G是不连通的，则可对G的每一分图重复上述证明，最后得出同样的结论。定理得证。

定义 8-15 设G是具有互补结点子集V_1和V_2的偶图，其中$V_1=\{v_1,v_2,\cdots,v_q\}$。$V_1$对$V_2$的**匹配**是$G$的一个子图，它由$q$条边$\{v_1,v_1'\}$，$\{v_2,v_2'\}$，$\cdots$，$\{v_q,v_q'\}$组成，其中$v_1',v_2',\cdots,v_q'$是$V_2$中$q$个不同的元素。

图 8-37 给出了一具有互补结点子集V_1和V_2的偶图和一V_1对V_2的匹配（用粗线表示）。

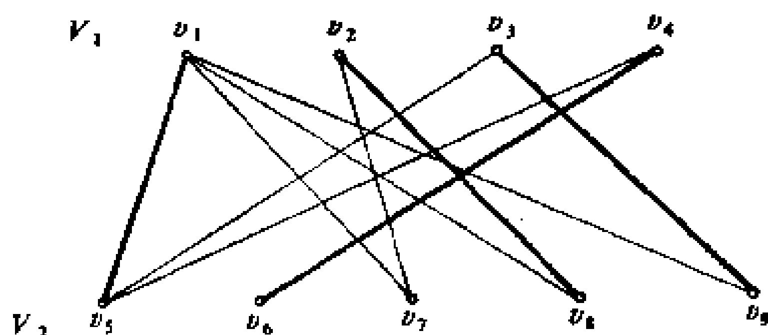


图 8-37

有不少实际问题可以化为在一个偶图中求匹配的问题。例如，有m个人和n件工作，每个人都只熟悉这n件工作中的某几件，每一件工作都需要一个人干，那么能不能将这n件工作都分配给熟悉它的人干呢？用一个偶图来表示这个问题，V_1中的结点代表人，V_2中的结点代表工作，当且仅当$u\in V_1$熟悉工作$v\in V_2$时，图中有边$\{u,v\}$。因此，我们的问题就是问：能否在此偶图中找到一个V_2对V_1的匹配。

显然，并不是所有的偶图都有匹配。一个偶图存在V_1对V_2的匹配的一个必要条件是$\#V_2\geqslant\#V_1$。但这个条件并不是充分的。图 8-38 中的偶图就是一个例子。

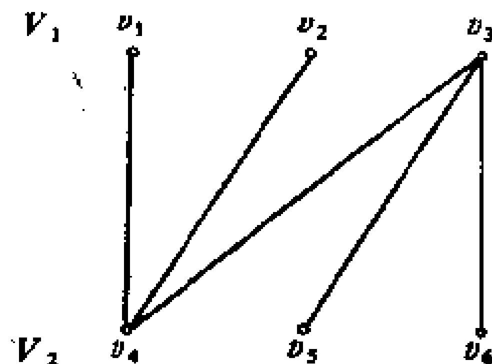


图 8-38

定理8-10 设G是具有互补结点子集V_1和V_2的一个偶图。则G中存在一V_1对V_2的匹配的充要条件是：V_1中每k个结点$(k=1,2,\cdots,\#V_1)$至少和V_2中k个结点相连接（该条件称为相异性条件）。

证明 令$\#V_1=q$，若G中存在一V_1对V_2的匹配，则V_1的q个结点分别和V_2中q个相异的结点相连接，因此相异性条件显然成立。

反之，设G满足相异性条件，我们将证明(对V_1的结点个数进行归纳)，一个V_1对V_2的匹配能被构造出来。

当$\#V_1=1$和$\#V_1=2$时，若相异性条件满足，则一V_1对V_2的匹配是显然存在的。

设对于$\#V_1=1,2,\cdots,q-1$，任何具有互补结点子集V_1和V_2的偶图，当相异性条件满足时，存在一个V_1对V_2的匹配，又设图G满足相异性条件，且$\#V_1=q$。

(i) 若V_1中每k个结点$(k=1,2,\cdots,q-1)$和V_2中多于k个结点相连接，则一V_1对V_2的匹配能如下法构造：指定任一边$\{v_i,v_j\}$(其中$v_i\in V_1$，$v_j\in V_2$)给匹配，显然，在具有互补结点子集$V_1-\{v_i\}$和$V_2-\{v_j\}$的偶图中，相异性条件仍然满足。因此，根据归纳假设，一匹配能被构造出来。该匹配和$\{v_i,v_j\}$一起即是所要寻找的V_1对V_2的匹配。

(ii) 若存在某正整数$k_0\leqslant q-1$，使得具有k_0个结点的一集合$U_1\subset V_1$，其中的结点和$U_2\subset V_2$中的恰好k_0个结点相连接。在此情况下，一V_1对V_2的匹配能如下法构造：首先，由于U_1中k_0个结点只与U_2中的结点相连接，且由已知图G满足相异性条件，因此，在具有互补结点子集U_1和U_2的偶图中，相异性条件满足。由归纳假设一U_1对U_2的匹配能被构造出来。现假设具有互补结点子集$U_1'=V_1-U_1$(其中$\#U_1'=q-k_0$)和$U_2'=V_2-U_2$的偶图不满足相异性条件，即有某$k\leqslant q-k_0$存在，使得某一k结点集$U_1''\subseteq U_1'$，

其中的结点仅和U_2'中$k'<k$个结点相连接。于是，集$U_1 \cup U_1''$是V_1中具有k_0+k个结点的一个子集，这些结点和V_2中$k_0+k'<k_0+k$个结点相连接，这和G满足相异性条件相矛盾。因而，具有互补结点子集U_1'和U_2'的偶图必满足相异性条件。因此，能构造出一个U_1'对U_2'的匹配。由于$V_1=U_1 \cup U_1'$，$V_2=U_2 \cup U_2'$，这就完成了一V_1对V_2的匹配的构造。定理证完。

下一定理给出了一偶图存在匹配的一个充分条件，但不是必要的。该条件对任意给出的偶图能极容易地进行检验，因而在考察较为复杂的相异性条件之前，可首先考察这个充分条件。

定理 8-11 设G是一具有互补结点子集V_1和V_2的偶图，则G具有V_1对V_2的匹配的充分条件是：存在某一整数$t>0$，

(i) 对V_1中的每个结点，至少有t条边与其相关联；

(ii) 对V_2中的每个结点，至多有t条边与其相关联。

证明 若(i)成立，则关联于V_1中具有k个结点($k=1,2,\cdots,\#V_1$)的任意子集的边的总数至少为kt。由(ii)，这些边至少必须关联于V_2中k个结点。于是V_1中的每k个结点($k=1,2,\cdots,\#V_1$)至少和V_2中的k个结点相连接。由定理8-10可知G有V_1对V_2的匹配。证完。

例如，图8-39的偶图满足定理8-11的条件(i)和(ii)，其中$t=3$。因此有匹配。

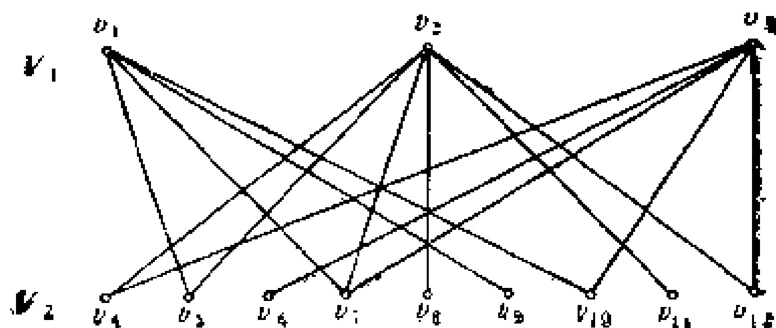


图8-39

定理8-11在实际生活中可与这样一个问题相联系，即“确定委员会主席的职位问题”。如图8-39中v_1, v_2, v_3可看作是三个委员会，因此$V_1=\{v_1, v_2, v_3\}$是三个委员会的集合，V_2中与$v_i(i=1,2,3)$相连接的结点可看作是该委员会的委员，现要为这三个委员会挑选3个主席，使得v_i的主席必须是v_i的委员，且不允许一个人兼任一个以上委员会的主席。这实际上就是寻找一个从委员会的集合V_1到所有委员会的委员的并集V_2的一个匹配。按照定理8-11，如果存在一整数$t>0$，使得每个委员会至少有t个委员，而每个人至多只能是t个委员会的委员，则委员会的主席职位问题是可以解决的。

§8.7 平面图

我们常将图用平面上的一个图解来表示，可以发现，将图画在平面上时允许边在结点之外的其他点相交将是方便的，有时甚至是必要的。我们称相交的边是**相互交叉的边**。例如图8-40(*a*)中边$\{v_1, v_4\}$与$\{v_2, v_3\}$交叉，边$\{v_1, v_5\}$与$\{v_2, v_3\}$、$\{v_3, v_4\}$分别交叉。

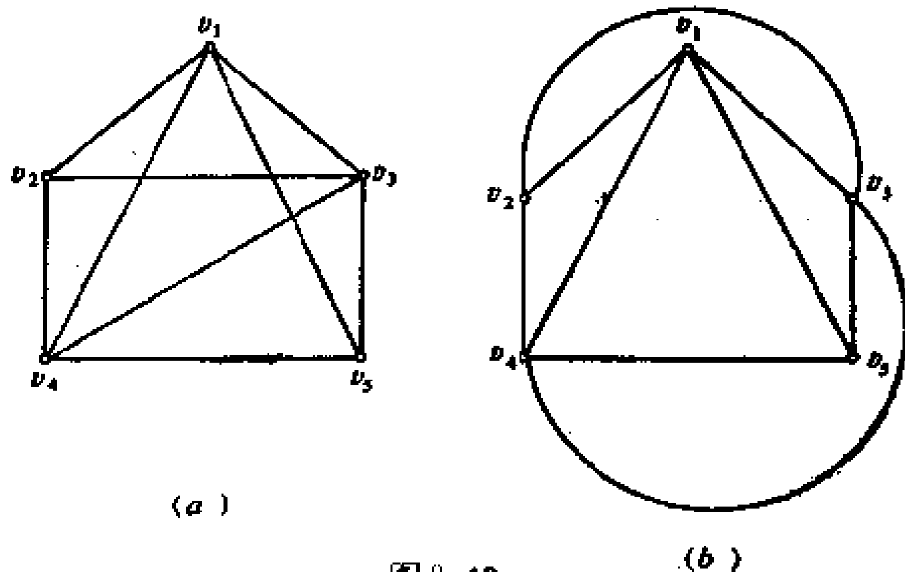


图8-40

定义 8-16 若一个图G能画于平面上而边无任何交叉，则称图G为**平面图**。否则称图G为**非平面图**。

图 8-40(a) 是平面图，因为它能画成如图 8-40(b) 所示，没有任何交叉。

显然，当且仅当一个图的每个分图都是平面图时，这个图是平面图。所以，在研究平面图的性质时，只要研究连通的平面图就可以了。我们约定本节中所谈的图都是连通的。

设G是画于平面上的一图，$\sigma = v_1 \cdots v_2 \cdots v_3 \cdots v_4 \cdots v_1$ 是G中的任一坏。$\alpha = v_1 \cdots v_3$ 和 $\alpha' = v_2 \cdots v_4$ 是G中任二无公共结点的真路（参见图8-41，它显示了各种可能的画法），可以看出，当且仅当α和α'两者都同在σ的内部或外部时，α与α'交叉。这一简单的事实对用观察法来证实一给出的图是非平面图时常是很有用的。

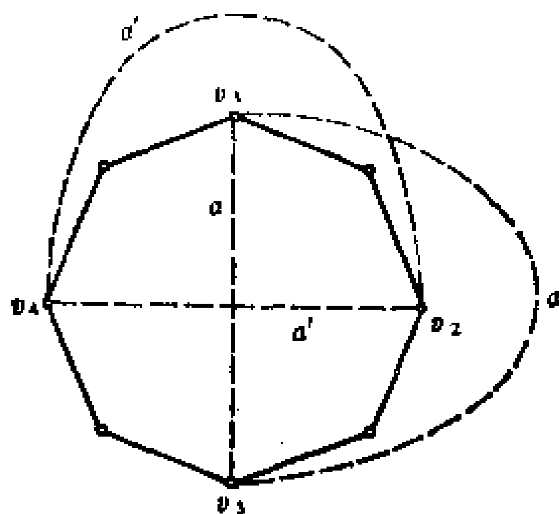


图 8-41

例如，一电路的组成如下：它有各包含三个结点的两个集合，其中一个集合的每一个结点将用导线和另一个集合的所有结点相连接（参见图 8-42(a)），问是否可以安置电路使导线互不交叉（避免交叉对“印刷电路”来说是有实际意义的）？显然，这个问题等价于判定图 8-42(a) 所示之图是否是一个平面图。注意到图中有一坏 $\sigma = v_1 v_6 v_3 v_5 v_2 v_4 v_1$ 和边 $\{v_1, v_5\}$，$\{v_6, v_2\}$ 及 $\{v_3, v_4\}$，

这些边的每一条要么在σ内，要么在σ外，因此这三条边中至少有两条在σ的同一边，因而这图是非平面图（参见图8-42(b)），故该电路无法安置为无交叉。

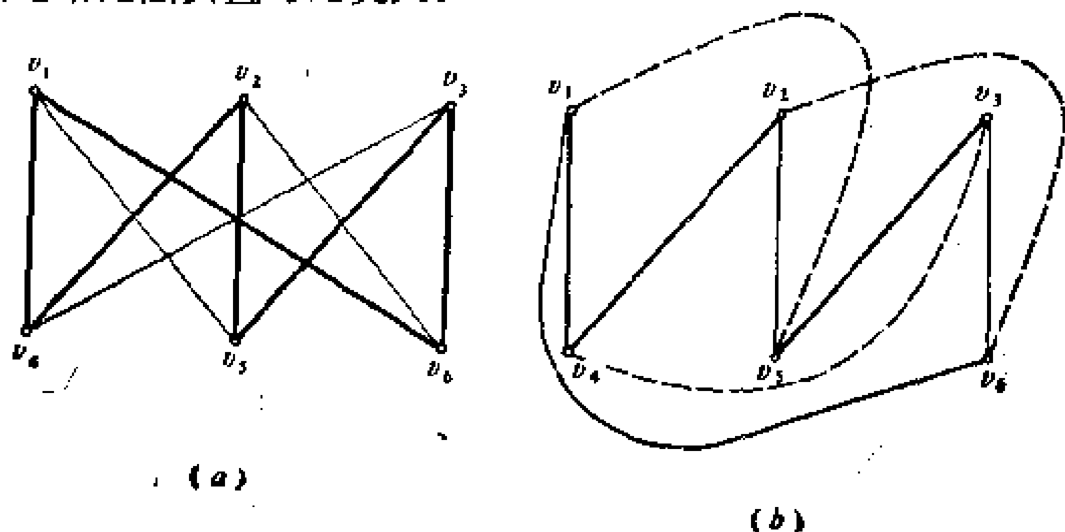


图8-42

设G是一个平面图，图的边所包围的一个区域，其内部既不含图的结点，也不含图的边，这样的区域称为G的一个**面**。面的边界就是包围该面的各边所构成的回路。如果面的面积是有限的，则称该面为**有限面**，如果面的面积是无限的，则称该面为**无限面**。对于每一个平面图，恰有一个无限面。若两个面的边界至少有一条公共边，则称这两个面是**相邻的**；否则称这两个面是**不相邻的**。

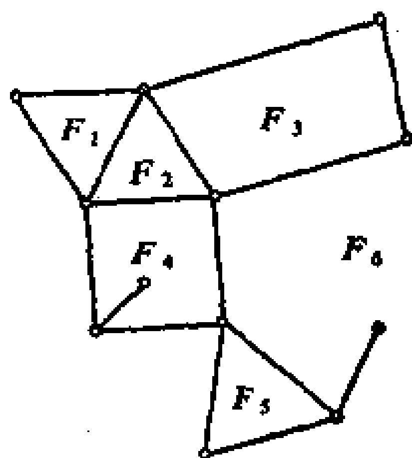


图8-43

例如图8-43中，面F_1与F_2，F_2与F_3是相邻的，但F_4与F_5是不相邻的。面F_6是无限面，其它的面都是有限面。

定理8-12 设G是一连通的平面图，则有

$$n-m+k=2。\qquad (8\text{-}1)$$

这里 n，m，k 分别是图 G 的结点数、边数和面数（包括无限面）。(8-1) 式称为对于平面图的欧拉公式。

证明 （对面数 k 进行归纳）

当 $k=1$ 时，G 中不含有环，故为一棵树，由定理8-6有 $m=n-1$，故有 $n-m+k=n-(n-1)+1=2$。定理成立。

设定理对有 $k-1$ 个面的所有连通的平面图成立，而 G 是有 k 个面的一个连通的平面图，$k\geqslant 2$，于是 G 至少有一个环。去掉 G 的一个环上的一条边 e，则 $G'=(V, E-\{e\})$ 是连通的，G' 有 $k-1$ 个面，$m-1$ 条边。由归纳假设 $n-(m-1)+(k-1)=2$，即 $n-m+k=2$，因此定理成立。

定理 8-13 在有两条或更多条边的任何连通的平面图 G 中，有

$$m\leqslant 3n-6.$$

证明 当 $m=2$ 时，因为 G 是简单图，必无环，所以 $n=3$，上式成立。

当 $m>2$ 时，我们计算每一个面的边界中的边数，然后计算各个面的边界的边数的总和。因为 G 是简单图，所以每个面由三条或更多条边围成。按照这样计算，各面的总边数大于或等于 $3k$。另一方面，因为一条边至多在两个面的边界中，所以上述计算的总边数小于或等于 $2m$。因此有 $2m\geqslant 3k$，即 $\frac{2}{3}m\geqslant k$。根据欧拉公式，我们有

$$n-m+\frac{2}{3}m\geqslant 2 \qquad (8\text{-}2)$$

或

$$m\leqslant 3n-6. \qquad (8\text{-}3)$$

证完。

利用上述结论，我们可以证明图8-44不是平面图。因为在这个图中，$n=5$，$m=10$，不满足(8-3)中的不等式。

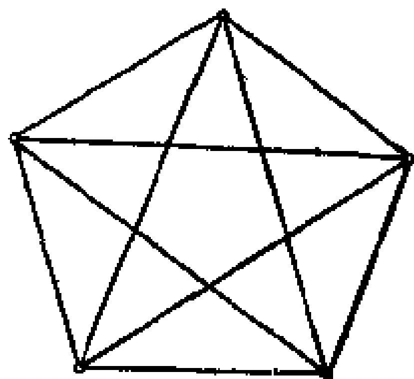


图8-44

同样可以证明，图8-45也不是平面图(注意，图8-45和图8-42表示同一个图)。因为，如果这个图是平面图，又由这个图是偶图，可知每个面必由4条或更多条边围成。因此，(8-2)式中的不等式变为

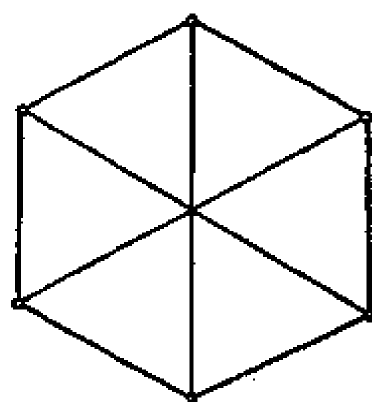


图8-45

$$n-m+\frac{m}{2}\geqslant 2$$

或

$$m\leqslant 2n-4. \tag{8-4}$$

但图8-45中，$n=6$，$m=9$，并不满足(8-4)中的不等式。

虽然欧拉公式有时可用来判定某一个图是非平面图，但在公式的这种应用中，对于包含较多的结点和边的图，这个证明将变得很复杂。下面叙述的库拉托斯基(Kuratowski)定理明确地给出了判定一个图是平面图的必要充分条件。

如果象图8-46(*a*)那样，在图的边上插入一个新的次数为2的结点，使一条边分成两条边，或者如图8-46(*b*)所示，对于两条关联于一个次数为2的结点的边，去掉这个结点，将两条边合并成一条边，图的平面性显然不受影响。由此我们给出下面的定

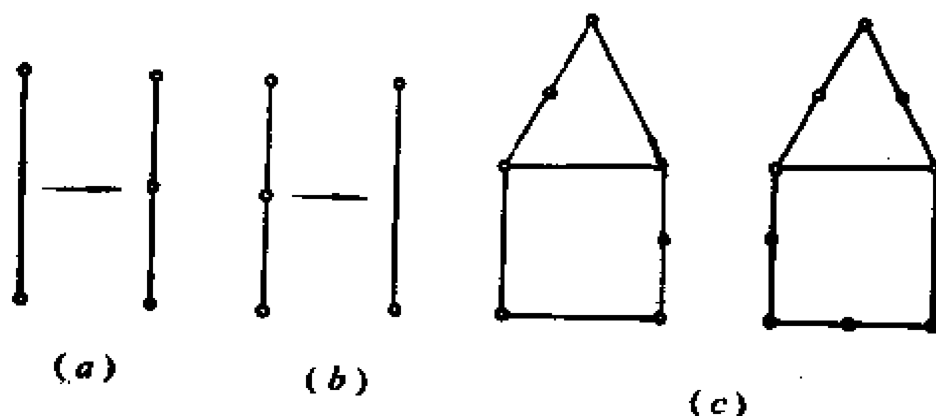


图8-46

义：如果两个图G_1和G_2，它们是同构的，或者通过反复插入和删除次数为2的结点，它们能变成同构的图，则称图G_1和G_2**在次数为2的结点内同构**。例如图8-46(c)的两个图是在次数为2的结点内同构的。

定理8-14 （Kuratowski定理）一个图是平面图的必要充分条件是它不包含任何在次数为2的结点内和图8-44中的图或图8-45中的图同构的子图。

这个定理的证明虽然是基本的，但是很长，故省略[注]。

构成一单个环的图称为**封闭折线**。一**封闭折线图**是一平面图，可归纳地定义如下：

（基础）一封闭折线是一封闭折线图。

（归纳步）设$G=(V,E)$是一封闭折线图，又设$\alpha=v_iv_{i_1}v_{i_2}\cdots v_{i_{l-1}}v_j$为不与$G$交叉的任一真路（长$l\geqslant1$），其中$v_i,v_j\in V$，但$v_{i_r}\notin V(r=1,2,\cdots,l-1)$，那么由$G$和$\alpha$组成的图，即图$(\bar{V},\bar{E})$，其中

$$\bar{V}=V\cup\{v_{i_1},v_{i_2},\cdots,v_{i_{l-1}}\},$$
$$\bar{E}=E\cup\{\{v_i,v_{i_1}\},\{v_{i_1},v_{i_2}\},\cdots,\{v_{i_{l-1}},v_j\}\},$$

也是一封闭折线图。

由封闭折线图的定义可知，它是一平面图（可能为多重图，因为长为2的环是允许的）。图8-47是一封闭折线图的例。

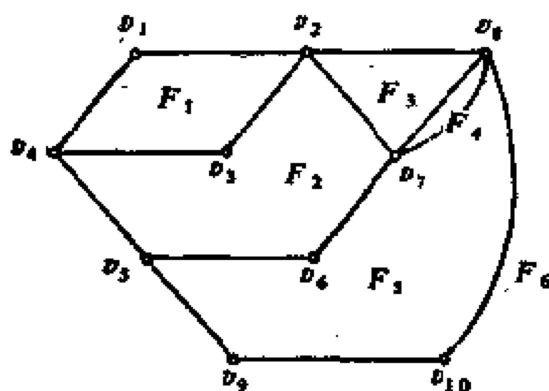


图8-47

给出一具有面$F_1,F_2,\cdots,F_k$（包括无限面）的封闭折线图G。G的**对偶图**

[注] Kuratowski定理的证明可参看：[法] C. 贝尔热著，李修睦译，《图的理论及其应用》，上海科学技术出版社（1963年）。

$\tilde{G}$ 是这样的图，它可由 G 按下法得到：对 G 的任一面 F_i 指定一结点 f_i 给 $\tilde{G}$，对 G 中 F_i 和 F_j 公共的每一条边，指定一边 $\{f_i, f_j\}$ 给 $\tilde{G}$。也就是画每一结点 f_i 于面 F_i 内，并用连接 f_i 和 f_j 的边分别交叉 F_i 和 F_j 的每一条公共边，便可得到 G 的对偶图 $\tilde{G}$。图 8-48 给出了一封闭折线图（实线）和它的对偶图（虚线）。由这种构成方法不难看出，每一封闭折线图的对偶图也必然是一封闭折线图。而且，若 $\tilde{G}$ 是 G 的对偶图，则 G 也是 $\tilde{G}$ 的对偶图。

用类似的方法也可定义平面图的对偶图。

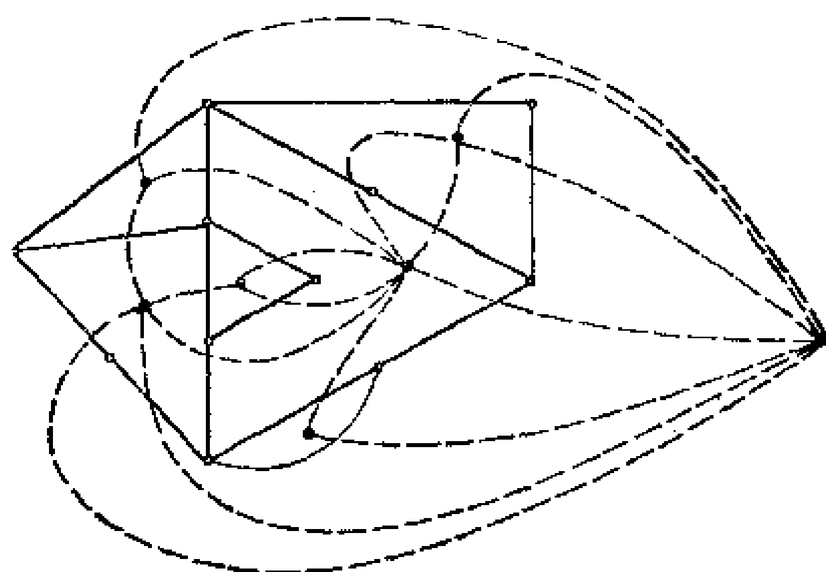


图 8-48

一图 G，若其对偶图 $\tilde{G}$ 同构于 G，则称其为**自对偶图**。图8-49 给出了一自对偶图的例。

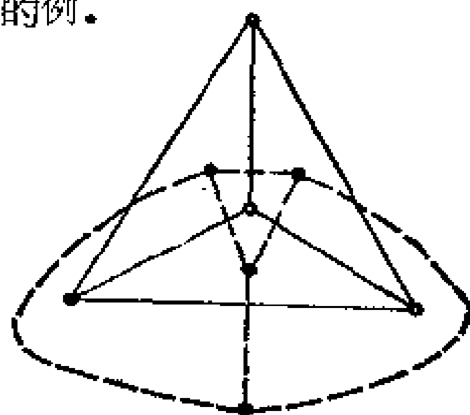


图 8-49

与封闭折线图有关的一著名问题是“4色猜想”问题，即每一封闭折线图能用4种不同的颜色来着色，使任何两个相邻的面（包括无限面）具有不同的颜色。这个问题提出于上一世纪中期，经过许多数学家的努力，终于在1976年为爱普尔（K. I. Appel），黑肯（W. Haken）和考西（J. Koch）利用电子计算机的帮助得到了证明。在探求这一问题证明的漫长过程中，获得了图论和有关领域中许多重要的成果。

§8.8 有向图

类似于无向图，这里所说的有向图是指简单有向图，即它既没有长度为1的环，又没有多重边。有向图和无向图的区别在于有向图中边集E是V中不同元素的**有序**对偶的集合。在图解上，我们用一个由结点v_i指向v_j的箭头表示边(v_i, v_j)，而用相反方向的箭头表示边(v_j, v_i)。例如，图8-13显示的是有向图$G=(V, E)$，其中$V=\{v_1, v_2, v_3, v_4\}$，$E=\{(v_1, v_2), (v_1, v_4), (v_4, v_1), (v_3, v_1), (v_3, v_2), (v_3, v_4)\}$。

和无向图一样，有向图也能用相应的邻接矩阵$A=[a_{ij}]_{n\times n}$表示，其中

$$a_{ij}=\begin{cases}1 & 若\ (v_i, v_j)\in E,\\ 0 & 否则.\end{cases}$$

但这里A不一定关于主对角线对称。例如，图8-13的有向图G的邻接矩阵是

$$A=\begin{pmatrix}0 & 1 & 0 & 1\\ 0 & 0 & 0 & 0\\ 1 & 1 & 0 & 1\\ 1 & 0 & 0 & 0\end{pmatrix}.$$

如果在有向图$G=(V,E)$的图解中，允许有长度为1的环出现，即允许E中有相同元素的有序对偶出现，则有向图$G=(V,E)$的图解表示实际上就是定义在结点集V上的二元关系E的关系图。G的邻接矩阵A就是结点集V上二元关系E的关系矩阵。

设G和G'是两个分别具有结点集V和V'的有向图，若存在一个双射h：$V\to V'$，当且仅当(v_i,v_j)是G的边时，$(h(v_i),h(v_j))$是G'的边，则称**G'同构于G**。如同无向图一样，同构的有向图除可能结点的标记不一样外，其他完全是相同的。

有向图中的**子图、真子图**和**生成子图**与无向图中的相应术语有完全相同的含意。

如§8.5中所指出的，若在无向图的**开路、回路、真路**和**环**的定义中，用“有向路”来代替“路”，我们就得到有向图中这些相应术语的定义。

在有向图中，若存在一条从结点v_i到结点v_j的有向路，则称从v_i到v_j是**可达的**。若从结点v_i到v_j是可达的，则从v_i到v_j的路中必有一条最短的路，我们称它为从v_i到v_j的**短程**。短程的长度称为是从v_i到v_j的**距离**，记作$d(v_i,v_j)$。对于有向图来说，从结点v_i到v_j是可达的，并不意味着从v_j到v_i是可达的，即使v_i和v_j是相互可达的，$d(v_i,v_j)$也不一定等于$d(v_j,v_i)$。

在一个有向图中，如果略去边的方向，将其看作无向图时它是连通的，则称这个有向图是**弱连通的**。如果任何两个结点v_i和v_j中至少有一个由另一个出发是可达的，则称这个有向图是**单向连通的**。如果任何两个结点v_i和v_j都是相互可达的，则称这个有向图是**强连通的**。显然，强连通的有向图是单向连通的，单向连通的有向图是弱连通的。为了简单起见，弱连通的有向图有时就称为是连通的。

例如，图8-50中(a)是强连通的；(b)是单向连通的，但不是强连通的；(c)是弱连通的，但不是单向连通的。

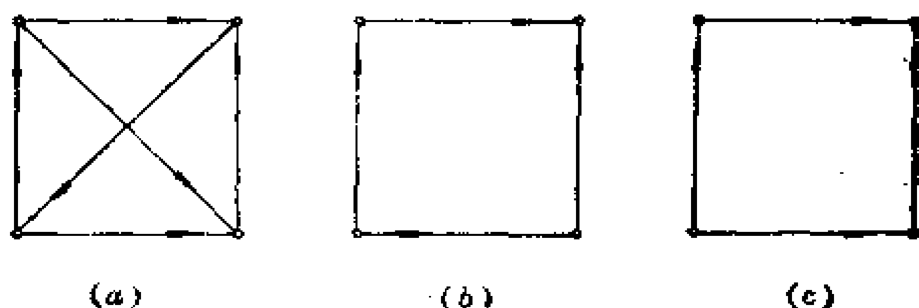

(a) (b) (c)

图 8-50

由连通性的不同定义，有向图 G 有三种类型的分图：**强分图**、**单向分图**和**弱分图**。它们分别是 G 中的极大强连通子图、极大单向连通子图和极大弱连通子图。不难看出，有向图的每一个结点和每一条边都恰处于一个弱分图中。但对于单向分图和强分图，情况就比较复杂。有向图的两个单向分图可能有公共的结点，也可能还有公共的边，而每个结点和每条边至少属于一个单向分图。例如，图8-51中的有向图有两个单向分图，它们的结点集分别为 $\{v_1, v_2, v_3\}$ 和 $\{v_1, v_3, v_4\}$。相反，一个有向图的两个强分图是没有公共结点的，每个结点都属于一个强分图。但可能有的边不属于任何强分图。图8-51的有向图有 4 个强分图，每个强分图都只有一个结点，从而每条边都不属于任何强分图。图8-52的有向图有 3 个强分图，它们的结点集分别为 $\{v_1, v_2, v_3, v_4\}$，$\{v_5, v_6, v_7, v_8\}$ 和 $\{v_9\}$。

对定理8-1和定理8-2的证明略作修改即可推广到有向图。

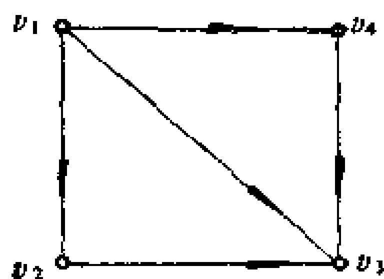


图 8-51

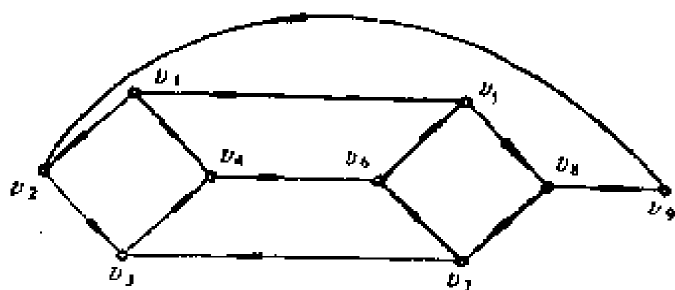


图 8-52

定理8-15 设G是具有结点集$V=\{v_1, v_2, \cdots, v_n\}$的有向图，且从结点$v_i$到$v_j$是可达的($v_i \neq v_j$)，则其短程是一条长度不大于$n-1$的真路。

推论 设G是具有n个结点的有向图，则G中任一环的长度不大于n。

定理8-16 设G是具有结点集$\{v_1, v_2, \cdots, v_n\}$和邻接矩阵$A$的有向图，则$A^l$ $(l=1, 2, \cdots)$的(i, j)项元素a_{ij}是从v_i到v_j长度为l的有向路的总数。

同样，定理8-3和定理8-4也可推广到有向图。

定理8-17 一个连通的有向图G具有欧拉回路的充要条件是G的每一个结点的引入次数和引出次数相等。一个连通的有向图G具有欧拉路的充要条件是除两个结点外，每一个结点的引入次数等于引出次数，对于这两个结点，一个结点的引入次数比它的引出次数大1，另一个结点的引入次数比引出次数小1。

在有向图中，两条边(v_i, v_j)和(v_j, v_i)称为边的一个**对称对**。没有对称对的有向图称为**定向图**。例如，将一个无向图G的各条边随意取定一个方向，就构成一个定向图。若$G=(V, E)$是一个有向图，且对于任意两个不同的结点$v_i, v_j \in V$，(v_i, v_j)和(v_j, v_i)中恰有一个在E中，则称G是一个**竞赛图**。一个无向完全图的定向是一个竞赛图。一有向图G的**真生成路**是指通过G的每个结点恰好一次的一条有向路。例如，图8-53中的路$v_4v_5v_3v_1v_2$是一真生成路。

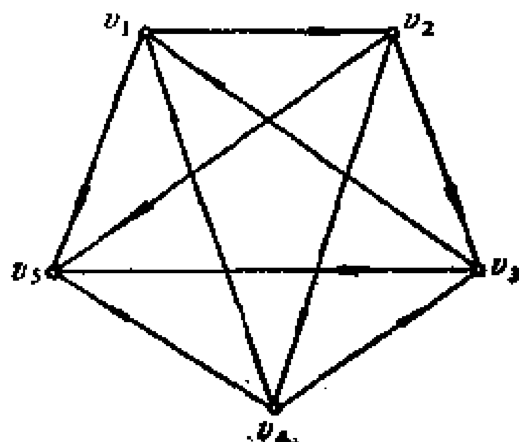


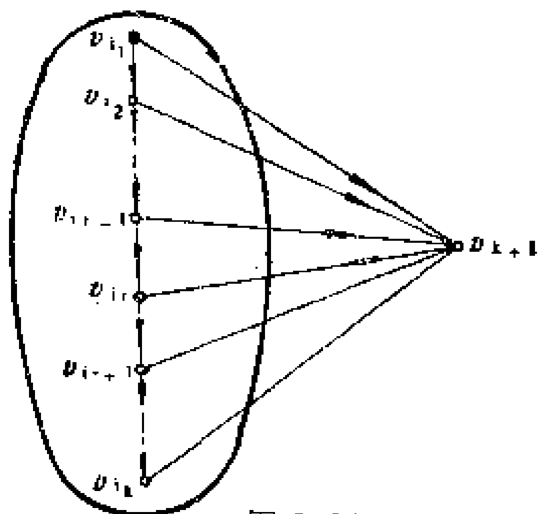
图8-53

定理8-18 每一竞赛图$G=(V, E)$有一真生成路。

证明 (对$\#V$进行归纳)

当$\#V=1$和$\#V=2$时，定理显然成立。

假设定理对所有 k 个结点的竞赛图都成立，并设 G 是一个具有结点集 $V=\{v_1, v_2, \cdots, v_{k+1}\}$ 的竞赛图。令 G_k 表示具有结点集 $V-\{v_{k+1}\}$ 的图 G 的竞赛子图。由归纳假设 G_k 有一真生成路，设为 $v_{i_1}v_{i_2}\cdots v_{i_k}(v_{i_1}, v_{i_2}, \cdots, v_{i_k}\in V-\{v_{k+1}\})$，那么，$G$ 或包含有边 (v_{k+1}, v_{i_1}) 或包含有边 (v_{i_1}, v_{k+1})。若是前一情况，则 $v_{k+1}v_{i_1}v_{i_2}\cdots v_{i_k}$ 是 G 的一真生成路。在后一情况下，令 r 是使 (v_{k+1}, v_{i_r}) 为 G 的一条边的最小整数，则 $v_{i_1}v_{i_2}\cdots v_{i_{r-1}}v_{k+1}v_{i_r}\cdots v_{i_k}$ 是 G 的一真生成路（参见图 8-54）。如果不存在这样的 r，则 $v_{i_1}v_{i_2}\cdots v_{i_k}v_{k+1}$ 是 G 的一真生成路。于是，在所有的情况下 G 有一真生成路。证完。


图 8-54

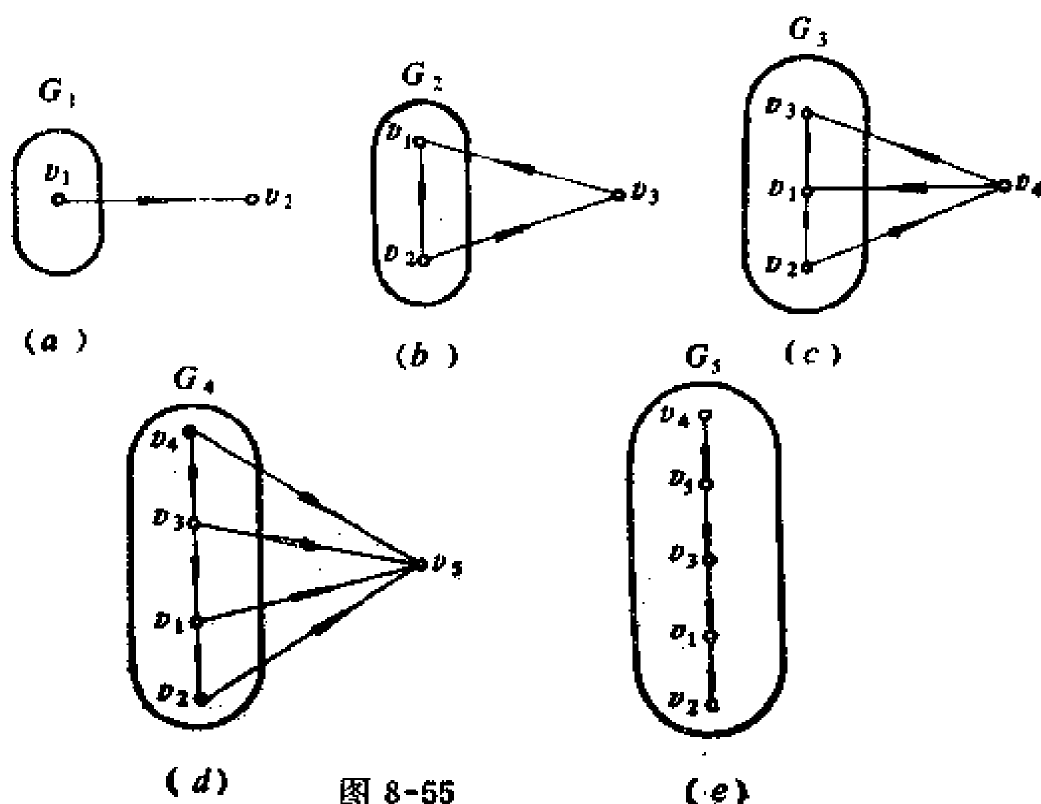


图 8-55

按照定理8-18的证明中所提供的方法，竞赛图8-53中的真生成路可如图8-55所示的步骤来决定。

具有 n 个结点的竞赛图，可以看作是 n 个选手，他们中的每个选手依次和其他每个选手进行某项比赛，选手 v_i 和 v_j 间的一场比赛，若 v_i 是优胜者，则由边 (v_i, v_j) 表示（不允许平局）。竞赛图中的一真生成路意味着有可能按某种次序列出 n 个选手的名次，例如图8-55中，该次序是 $v_4v_5v_3v_1v_2$，即 v_4 是最好的选手。但这样推出的结论是不合理的，因为它没有考虑选手取胜的次数。例如 v_2 取胜 3 次，v_5 仅取胜一次，但 v_5 却被认为是比 v_2 好的选手。

习 题

1. 图8-56所示之图是否同构于图8-5？

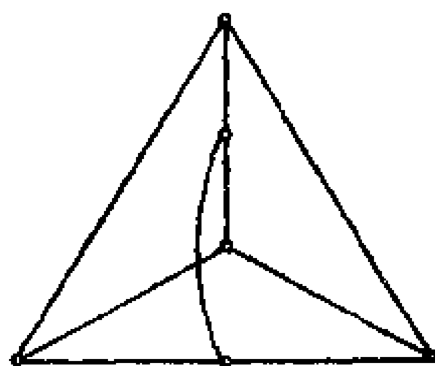


图 8-56

2. 图8-57中所给出的两个 8 结点图是否同构？证明你的回答。

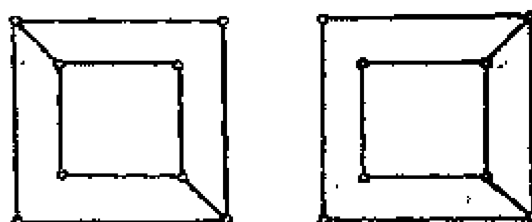


图 8-57

3. 证试明在任何图中奇次数结点的个数是偶数。

4. 设G是具有 4 个结点的完全图。

(1) G 有多少个子图？

(2) G 有多少个生成子图？

(3) 如果没有任何两个子图是同构的，则G的子图个数是多少？请将这些子图构造出来。

5. 在图8-58中找出其所有的真路和环。该图是否包含有分离边？

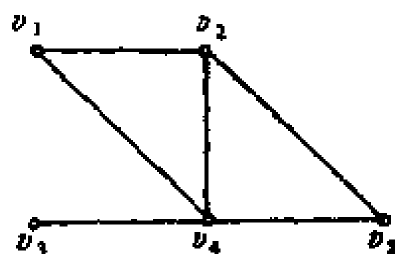


图 8-58

6. 图G由邻接矩阵

$$A=\begin{pmatrix} 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

给出，G是否是连通的？

7. 试证明：图G的任一条边，若其不是分离边，则必出现于G中的某一环里。

8. 试证明：若图G的每一结点的次数为 2，则G的每一分图均将包含一环。

9. 若图G的补图同构于G，则称G为自补图。试证明图8-59是自补图。你能否找到其它 5 结点的自补图？

10. 设A为具有n个结点的图G的邻接矩阵。试证明：若G有哈密顿环，则A^n的主对角线非零。并证明该命题的逆命题并不成立。

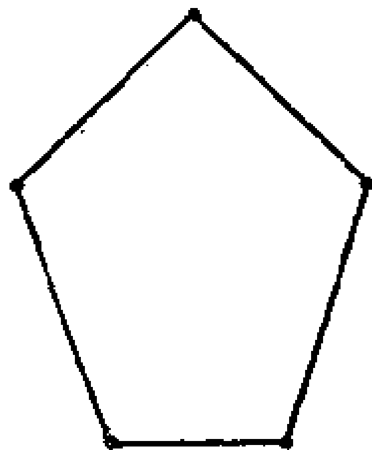


图 8-59

11. 已知关于人员 a, b, c, d, e, f 和 g 的下述事实：

a 说英语；

b 说英语和西班牙语；

c 说英语、意大利语和俄语；

d 说日语和西班牙语；

e 说德语和意大利语；

f 说法语、日语和俄语；

g 说法语和德语。

试问：上述七人中是否任意两人都能交谈（如果必要，可由其余五人中所组成的译员链帮忙）？

12. 试从图8-60中找出一条欧拉回路。

13. 试从图8-61中找出一条欧拉路。

14. 图8-62显示了4个图，试判定哪个是欧拉图，哪个是哈密顿图。在各适当情况下指出欧拉回路和哈密顿环。

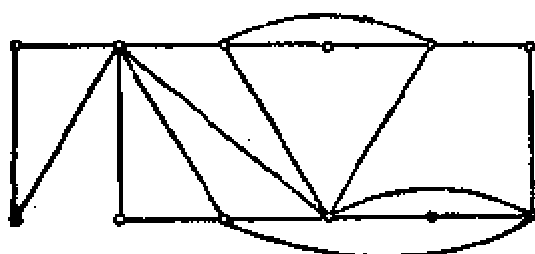


图 8-60

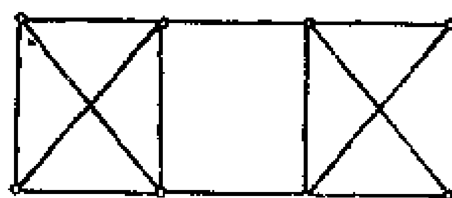
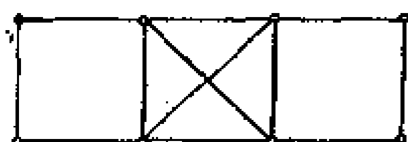
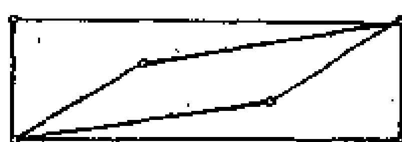
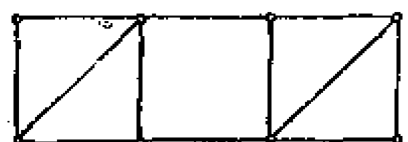


图 8-61







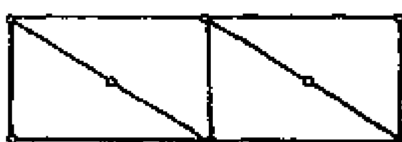


图 8-62

15。某流动售货员居住在a城，打算走销b,c,d城后返回a城。若该四城间的距离如图8-63所示，试找出完成该旅行的最短路线。

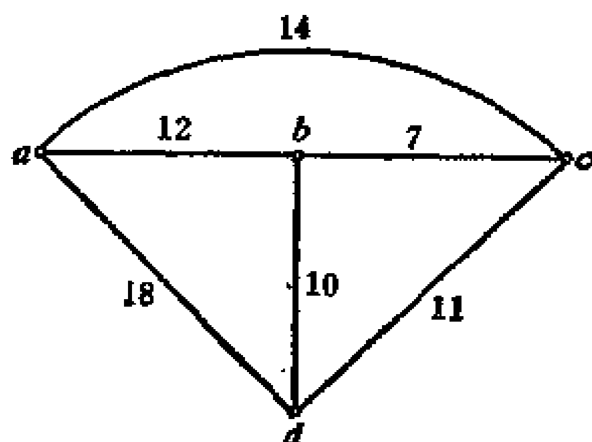


图 8-63

16。构造互不同构的所有五结点的树。

17。试证明当且仅当图G中的每一条边均为分离边时，图G是树林。

18。设G是一连通图，其中边e关联于结点v。试证明若v的次数为1，则G的每一生成树均包含e。

19。试证明连通图G的任一边是G的某一生成树的枝。

20。证明或反驳下一结论：连通图G的任一边为G的某一生成树的弦。

21。试证明具有m条边的连通图最多具有$m+1$个结点。

22。n个结点的完全图的环秩是多少？

23。构造图8-64的生成树，它的环秩是多少？

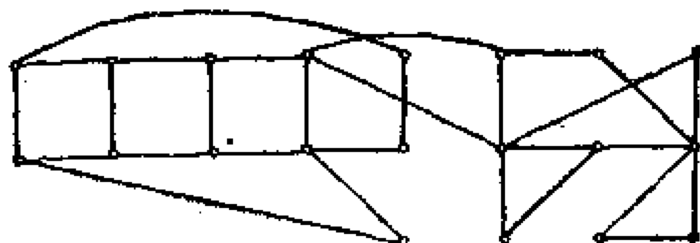


图 8-64

24. 分别用先根、中根和后根的次序通过图 8-31 中的二元树 T'。

25. 用二元树表示图8-29(a)中的有向树。

26. 试举例说明：仅一个结点的引入次数是 0，而其它所有结点的引入次数是 1 的有向图不一定是有向树。

27. 根据有向图的邻接矩阵，如何确定它是否是有向树？如果它是有向树，如何确定它的根和终止结点？

28. 已知关于人员 a,b,c,d,e 和 f 的下述事实：

a 说汉语、法语和日语；

b 说德语、日语和俄语；

c 说英语和法语；

d 说汉语和西班牙语；

e 说英语和德语；

f 说俄语和西班牙语。

试问：能否将这六个人分成两组，使同一组中没有两个人能互相交谈？

29. 图8-65是否为偶图？若是，找出它的互补结点集。

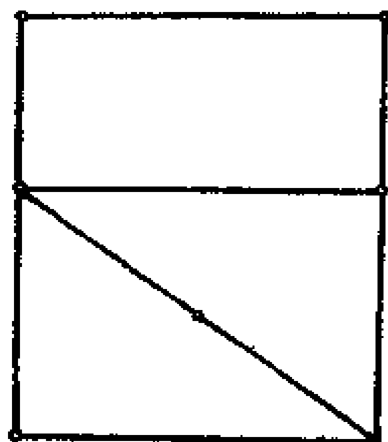


图 8-65

30. 对图8-66所示之偶图

(1) 说明"t 条件"(定理8-11)是满足的。

(2) 说明"相异性条件"(定理8-10)是满足的。

(3) 构造一 V_1 对 V_2 的匹配。

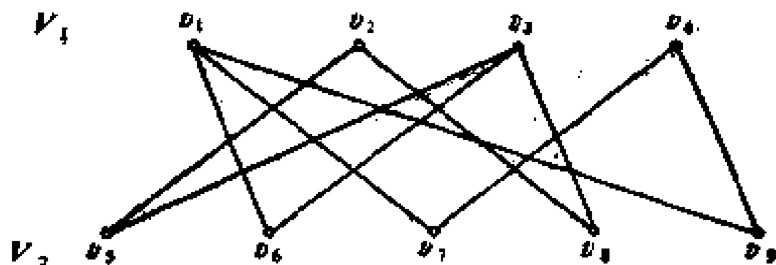


图 8-66

31. 画出六个结点的所有非平面图，使没有两个图是相互同构的。

32. 用定理8-14证明图8-67是非平面图。

33. 构造图8-68所示之图的对偶图。

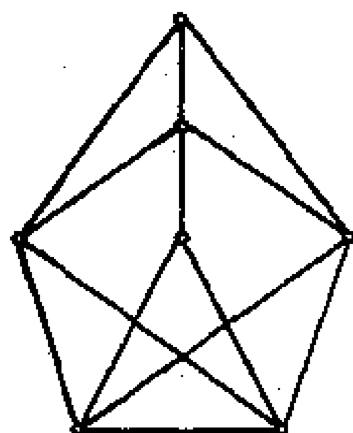


图 8-67

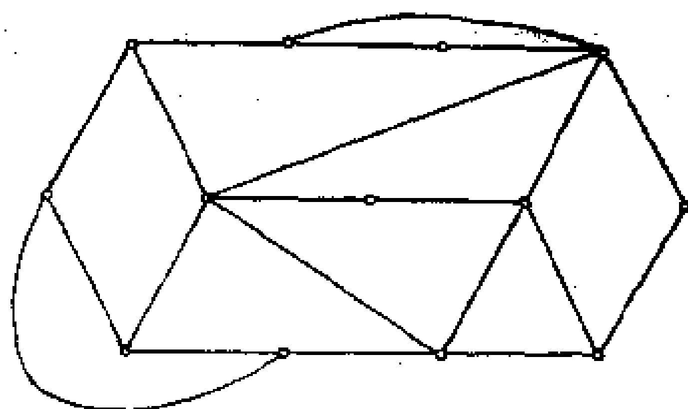


图 8-68

34. 试证明若一 (n, m) 图是自对偶的，则 $m = 2(n-1)$。

35. 用 3 种颜色着色图8-69之图，使没有两相邻的面(包括无限面)具有相同的颜色。

36. 在图8-70所示之竞赛图中找出一真生成路。

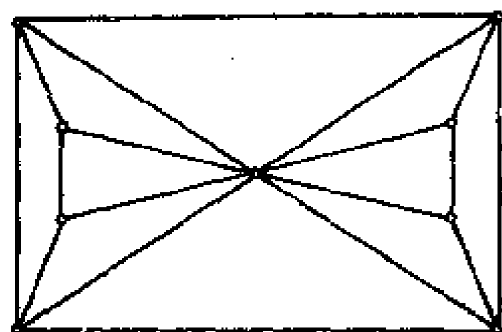


图 8-69

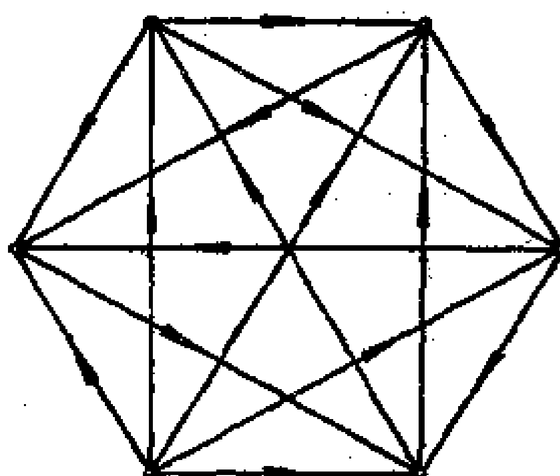


图 8-70

第九章　数理逻辑

数理逻辑是用数学的方法研究思维规律的一门学科。由于它使用了一套符号简洁地表达出各种推理的逻辑关系，因此数理逻辑一般又称为符号逻辑。数理逻辑和电子计算机的发展有着密切的联系，它为机器证明、自动程序设计、计算机辅助设计等计算机应用和理论研究提供必要的理论基础。

在这一章里，我们介绍数理逻辑最基础的内容，从自然推理的角度介绍命题演算和谓词演算两个部分。

（一）命题演算

§9.1　命题和命题公式

语言的单位是句子。句子可以分为疑问句、祈使句、感叹句与陈述句等，其中只有陈述句能分辨真假。别种句子（如疑问句、祈使句等）无所谓真假。在数理逻辑中，我们把每个能分辨真假的陈述句称作是一个**命题**。习惯上，命题用大写的拉丁字母A、B、…，P、Q、…或者带有下标的大写字母来表示。例如，下面的三个句子都是命题，可分别用A、B和C表示。

A：海洋的面积比陆地的面积大。

B：三角形的三内角和小于180°。

C：$2+2>5$。

以上这些语句的内容虽然各不相同，但它们都可以分辨其真

假。例如，命题A是正确的，也就是“真”的，而命题B和C都是不正确的，也就是“假”的。

我们用真值来描述命题是真或是假。如果一个命题是真的，我们就说它的真值为真，用“1”表示；如果一个命题是假的，我们就说它的真值是假，用“0”表示。

需要提醒注意的是，一个句子本身是否能分辨真假与我们是否知道它的真假是两回事。也就是说，对于一个句子，有时我们可能无法判断它的真假，但这个句子本身却是有真假的。例如，“1962年2月3日晚武汉市新华电影院曾放映了国产故事片‘白毛女’”。这是对过去的事情进行的判断，虽然我们一时很难分辨它的真假，但这句话本身是有其真假的。如果能查到当天武汉市的报纸，那么这句话正确与否就不难确定了。

正如前面所说，并非所有的句子都是命题。例如，下面的句子都不是命题：

(1) 你到哪里去？

(2) 你快起来跟我走吧。

(3) 啊，我的天哪！

前面所列举的三个命题都是最简单的命题。在语言学中，它们都是简单句。在数理逻辑中，将它们称作是**原子命题**（或原始命题）。有些命题是由几个简单句通过连接词构成一个复合句来表达的。这种做法和由两个数通过加、减、乘、除等运算而构造出一个新数，由两个集合通过并或交等运算而构造出一个新集合一样，构造新句子时所使用的运算就是语法中的连接词。例如

D：他既会跳舞，又会唱歌。

E：我唱歌或者跳舞。

F：如果你去教室，那么我就留在宿舍。

G：m^2是偶数当且仅当m是偶数。

都是一些用复合句表述的命题。在上面的例中，使用了连接词

既……又……

或者……或者……

如果……，那么……

……当且仅当……

下面我们定义五种**命题联结词**(或称命题的五种运算)。我们将会看到，它们和通常语言里的连接词是有所不同的，它们是通常语言里的连接词的逻辑抽象。若干个原子命题通过命题联结词而构成的新命题称作是**复合命题**。

1. **否定**“$\neg$”

设P是一个命题，利用“$\neg$”和P组成的复合命题称为命题P的**否命题**，记作“$\neg P$”。当命题P取值为真时，命题$\neg P$取值为假；当命题P取值为假时，命题$\neg P$取值为真。“$\neg P$”读作“非P”，“$\neg$”相当于普通语言中的“非”。例如，对于前面的命题A，命题$\neg A$为“海洋的面积不比陆地的面积大”。而命题C的否命题$\neg C$为“$2+2\leqslant5$”。否命题$\neg P$的取值也可用如下的一个表来定义，这种表称为否命题$\neg P$的“真值表”(真值表的构造类似于集合的成员表)。

P	$\neg P$
0	1
1	0

表中的“1”和“0”分别表示标记该列的命题取值为真和为假。

2. **合取**“$\wedge$”

设P和Q是两个命题，从P、Q利用“$\wedge$”组成的复合命题，记作“$P\wedge Q$”(读作“P且Q”)，称为**合取式复合命题**。$P\wedge Q$的取值情况是：当且仅当命题P和Q均取值为真时，$P\wedge Q$才取值为真。因此$P\wedge Q$的真值表如右边所示。

P	Q	$P\wedge Q$
0	0	0
0	1	0
1	0	0
1	1	1

“$\wedge$”是通常语言中“并且”、“既……又……”的逻辑抽象。

例如，我们用 D_1 和 D_2 分别表示命题"他会跳舞"和"他会唱歌"，则前面的命题 D 就是 $D_1 \wedge D_2$。

3. **析取"$\vee$"**

从命题 P 和 Q 利用"$\vee$"组成的复合命题，记作"$P \vee Q$"（读作"P 或 Q"），称为**析取式复合命题**。$P \vee Q$ 的取值情况是：当且仅当 P 和 Q 至少有一个取值为真时，$P \vee Q$ 便取值为真。因此 $P \vee Q$ 的真值表如右边所示。

P	Q	$P \vee Q$
0	0	0
0	1	1
1	0	1
1	1	1

例如，我们用 E_1 和 E_2 分别表示命题"我唱歌"和"我跳舞"，则前面的命题 E 就是 $E_1 \vee E_2$。

通常语言中的"或者"一词有不可兼的意思。例如，"我到北京出差或者到广州去度假"表示的是二者只能居其一，不会同时成立。按照联结词"$\vee$"的定义，当 P、Q 都为真时，$P \vee Q$ 也为真，因此，"$\vee$"所表示的"或"是"相容或"，对于"不可兼的或"，在数理逻辑中用联结词"$\veebar$"表示，称作"异或"或者"排斥或"。命题 $P \veebar Q$ 的取值情况是：当且仅当命题 P 和 Q 的真值相异时，$P \veebar Q$ 为真。若用 P 表示"我到北京出差"，Q 表示"我到广州度假"，则上一例句可表示为 $P \veebar Q$。但上一例句也可以不用联结词 $\veebar$ 而用 $\vee$ 表示为 $(P \wedge \neg Q) \vee (\neg P \wedge Q)$。

4. **蕴含"$\rightarrow$"**

从命题 P 和 Q 利用"$\rightarrow$"组成的复合命题，记作"$P \rightarrow Q$"（读作"如果 P，则 Q"），称为**蕴含式复合命题**。其中 P 称为蕴含式的前件，Q 称为蕴含式的后件。当前件 P 为真，后件 Q 为假时，命题 $P \rightarrow Q$ 取值为假，否则 $P \rightarrow Q$ 取值为真。$P \rightarrow Q$ 的真值表如右边所示。

P	Q	$P \rightarrow Q$
0	0	1
0	1	1
1	0	0
1	1	1

例如，如果我们用 F_1 和 F_2 分别表示命题"你去教室"和"我留在宿舍"，则命题 F 就是 $F_1 \to F_2$。

当前件 P 为真后件 Q 也为真时，复合命题 $P \to Q$ 为真，这在通常语言的意义下是正确的。即从前提条件 P 可以推出结论 Q 成立。如果前件 P 为真而后件 Q 为假，那么 $P \to Q$ 为假，这在通常语言的意义下也是正确的。它说明由前提条件 P 不能推出结论 Q 成立。按照我们的定义，当前件 P 为假时，不论后件 Q 是真还是假，命题 $P \to Q$ 总是真。这样的定义方式反映了客观实际。例如，若要我们证明命题"若 $a+2>10$，则 $a>8$"是正确的。我们的证明方法是在假设不等式 $a+2>10$ 成立的条件下，利用不等式的性质得出 $a>8$ 的结论，因而断定该命题是正确的。而对于 $a+2 \leqslant 10$ 的情形根本不予考虑，这无异乎是认为当前提条件 $a+2>10$ 不成立时，该命题为真。

5. **等值"$\longleftrightarrow$"**

从命题 P、Q 利用"$\longleftrightarrow$"组成的复合命题，记作 $P \longleftrightarrow Q$（读作"P 当且仅当 Q"），称为是**等值式复合命题**。它的真值表如右边所示。

P	Q	$P \longleftrightarrow Q$
0	0	1
0	1	0
1	0	0
1	1	1

从真值表可以看出，当且仅当命题 P 和 Q 取相同的值时，命题 $P \longleftrightarrow Q$ 才取值为真。例如，如果我们用 G_1 和 G_2 分别表示命题"m^2 是偶数"和"m 是偶数"，则命题 G 就是 $G_1 \longleftrightarrow G_2$。

在通常的语言中，用连接词连接的两个陈述句在内容上总是存在着某种联系，也就是整个语句总是有意义的。然而在数理逻辑中，关心的是复合命题与构成复合命题的各原子命题之间的真值关系，即抽象的逻辑关系，并不关心各语句的具体内容。因此，内容上毫无联系的两个命题也能组成具有确定真值的复合命题。例如，"如果 $2+3=5$，则武汉市是湖北省的省会。""$2+3=5$ 并且广州不是一个城市。"都是具有确定真值的命题。

由上我们看到，从已知命题通过使用 $\neg$、$\wedge$、$\vee$、$\rightarrow$、$\leftrightarrow$ 这五种逻辑联结词可以构造出新的命题。反复使用这些联结词可以产生出更加复杂的命题。例如

$$A\rightarrow(B\vee C),\quad A\rightarrow(B\rightarrow A),$$

$$\neg(P\leftrightarrow Q),\quad (\neg A\wedge\neg B)\rightarrow(C\wedge(D\vee E)).$$

在这些复合命题中，我们使用了括号表示连续使用的联结词执行的先后次序。我们规定，在各种联结词中联结词“$\neg$”最为优先，而且总是从最内层括号的运算作起。

下面我们举几个例子说明通常的语言如何**翻译成复合命题**。

例 1 “如果你走路时看书，那么你一定会成为近视眼。”

令 P 表示“你走路”，Q 表示“你看书”，R 表示“你是近视眼”，则上述语句可表示为

$$(P\wedge Q)\rightarrow R.$$

例 2 “除非他以书面或口头的方式正式通知我，否则我不参加明天的会议。”

令 P 表示“他书面通知我”，Q 表示“他口头通知我”，R 表示“我参加明天的会议”，则上述语句可表示为

$$(P\vee Q)\leftrightarrow R.$$

一个给定的命题或为真或为假，因此它具有确定的真值。一个任意的且真值不确定的命题，我们称它为**命题变元**。仍用大写字母表示。命题变元虽然没有确定的真值，但当我们进行解释，即用一个具体的命题代入时，它的真值就可得到确定。由于每一命题都只有“真”、“假”两种取值的可能性，因此为了简单起见，往往在对一个命题变元进行代入时，我们就直接以“真”或“假”为值代入，而不必代入具体的命题。

由命题变元、命题联结词和圆括号所组成的符号串可构成一命题公式。但并不是由这三类符号所组成的每一符号串都可成为命题公式。下面给出**命题公式**（或简称**公式**）的递归定义：

(1) 0、1 是命题公式；

(2) 命题变元是命题公式；

(3) 如果 A 是命题公式，则 $\neg A$ 是命题公式；

(4) 如果 A 和 B 是命题公式，则 $(A \vee B)$、$(A \wedge B)$、$(A \rightarrow B)$、$(A \leftrightarrow B)$ 也是命题公式。

(5) 只有有限次地利用上述 (1)、(2)、(3)、(4) 而产生的符号串才是命题公式。

为简单起见，我们常省去公式最外层的括号。例如，公式 $((\neg P \wedge Q) \leftrightarrow Q)$ 可写为 $(\neg P \wedge Q) \leftrightarrow Q$。

按照上述定义，下面的符号串是公式：

$$(P \vee Q) \rightarrow (\neg (Q \wedge R)), \quad \neg (P \vee R),$$

$$((R \wedge Q) \vee P) \leftrightarrow (Q \vee P).$$

下面的符号串不是公式：

$$P \rightarrow QP, \quad \vee R \rightarrow P, \quad P \rightarrow (Q \rightarrow R.$$

如果对五个命题联结词，规定它们结合力的强弱次序为：$\neg$、$\wedge$，$\vee$，$\rightarrow$，$\leftrightarrow$，则也可以省掉命题公式中的某些括号。但我们这里不这样作。

当公式中的每一个命题变元都被赋以确定的真值时，公式的值也就被确定了，从而成为一个命题。公式中所有命题变元的一组确定的取值称为公式的一组**真值指派**。含有 n 个命题变元的公式有 2^n 组不同的真值指派，对于每一组真值指派，公式都有一个确定的真值。公式与其命题变元之间的真值关系，可以用作真值表的方法表示出来（其构造方法类似于集合的成员表）。

例如，命题公式 $(P \rightarrow Q) \leftrightarrow (\neg P \vee Q)$ 的真值表如右表。

P	Q	$\neg P$	$\neg P \vee Q$	$P \rightarrow Q$	$(P \rightarrow Q) \leftrightarrow (\neg P \vee Q)$
0	0	1	1	1	1
0	1	1	1	1	1
1	0	0	0	0	1
1	1	0	1	1	1

又如，命题公式$(P\leftrightarrow Q)\wedge(\neg Q\rightarrow S)$的真值表为

P	Q	S	$P\leftrightarrow Q$	$\neg Q$	$\neg Q\rightarrow S$	$(P\leftrightarrow Q)\wedge(\neg Q\rightarrow S)$
0	0	0	1	1	0	0
0	0	1	1	1	1	1
0	1	0	0	0	1	0
0	1	1	0	0	1	0
1	0	0	0	1	0	0
1	0	1	0	1	1	0
1	1	0	1	0	1	1
1	1	1	1	0	1	1

一个命题公式，如果对于它所包含的命题变元的任何一组真值指派，取值恒为真，则称这样的公式为**重言式**. 重言式常用“1”表示. 相反，若对于它所包含的命题变元的任何一组真值指派，取值恒为假，则称这样的公式为**矛盾式**. 矛盾式常用“0”表示. 如果至少有命题变元的一组真值指派使得公式的值为真，则称这样的命题公式为**可满足的公式**. 例如，命题公式$(P\rightarrow Q)\leftrightarrow(\neg P\vee Q)$是重言式，命题公式$(P\leftrightarrow Q)\wedge(\neg Q\rightarrow S)$既不是重言式也不是矛盾式，它是一个可满足的公式.

如何判断一个命题公式是否为重言式呢？我们当然可以象前面那样列出它的真值表，看它的取值是否恒为真. 但是当公式很复杂或所含命题变元很多的时候，用列真值表的方法工作量太大，所以我们需要寻求另外一些切实可行的方法.

§9.2 命题公式的等值关系和蕴含关系

命题公式之间常有一些关系，比较基本的一种关系就是所谓等值关系.

设A和B是两个命题公式，$P_1,P_2,\cdots,P_n$是在A和B中出现

的全部命题变元。如果对于命题变元 $P_1, P_2, \cdots, P_n$ 的任意一组真值指派，公式 A 和 B 的取值都相同，则称公式 A 和 B 是**等值的公式**，表示为 $A \Leftrightarrow B$。

显然，当且仅当 A 和 B 的真值表完全相同时，A 和 B 是等值的公式。例如，P 和 $\neg(\neg P)$ 等值；$P \vee P$ 和 P 等值；$P \wedge \neg P$ 和 $Q \wedge \neg Q$ 等值。

注意"$\Leftrightarrow$"和"$\leftrightarrow$"是两个完全不同的符号。"$\Leftrightarrow$"不是命题联结词而是公式间的关系符号，$A \Leftrightarrow B$ 不表示一个公式，即不代表命题，它表示公式 A 和公式 B 有等值关系。而"$\leftrightarrow$"是命题联结词，$A \leftrightarrow B$ 是一个公式，表示某个命题。然而这两者之间有密切的联系，即 $A \Leftrightarrow B$ 的充要条件是公式 $A \leftrightarrow B$ 为重言式。

显然，公式之间的等值关系有如下三条性质：

(1) 自反性：对任意的公式 A，有 $A \Leftrightarrow A$。

(2) 对称性：对任意的公式 A、B，若 $A \Leftrightarrow B$，则 $B \Leftrightarrow A$。

(3) 可传递性：对任意的公式 A、B、C，若 $A \Leftrightarrow B$，$B \Leftrightarrow C$，则 $A \Leftrightarrow C$。

表 9-1 中列出了一些最重要的等值式，这些等值式也称作定律。其正确性均可以用真值表加以证明。下面仅举一例。

例 1 证明德·摩根定律 $\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$。

证明 列出公式 $\neg(P \vee Q)$ 和公式 $\neg P \wedge \neg Q$ 的真值表：

P	Q	$P \vee Q$	$\neg P$	$\neg Q$	$\neg P \wedge \neg Q$	$\neg(P \vee Q)$
0	0	0	1	1	1	1
0	1	1	1	0	0	0
1	0	1	0	1	0	0
1	1	1	0	0	0	0

由于真值表中公式 $\neg(P \vee Q)$ 与公式 $\neg P \wedge \neg Q$ 所标记的列完全相同，因此有 $\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$。

表 9-1

E_1	$P\vee Q\Leftrightarrow Q\vee P$	交换律
E_1'	$P\wedge Q\Leftrightarrow Q\wedge P$	
E_2	$(P\vee Q)\vee R\Leftrightarrow P\vee(Q\vee R)$	结合律
E_2'	$(P\wedge Q)\wedge R\Leftrightarrow P\wedge(Q\wedge R)$	
E_3	$P\wedge(Q\vee R)\Leftrightarrow(P\wedge Q)\vee(P\wedge R)$	分配律
E_3'	$P\vee(Q\wedge R)\Leftrightarrow(P\vee Q)\wedge(P\vee R)$	
E_4	$P\vee 0\Leftrightarrow P$	同一律
E_4'	$P\wedge 1\Leftrightarrow P$	
E_5	$P\vee\neg P\Leftrightarrow 1$	互否律
E_5'	$P\wedge\neg P\Leftrightarrow 0$	
E_6, E_6'	$\neg(\neg P)\Leftrightarrow P$	双重否定律
E_7	$P\vee P\Leftrightarrow P$	等幂律
E_7'	$P\wedge P\Leftrightarrow P$	
E_8	$P\vee 1\Leftrightarrow 1$	零一律
E_8'	$P\wedge 0\Leftrightarrow 0$	
E_9	$P\vee(P\wedge Q)\Leftrightarrow P$	吸收律
E_9'	$P\wedge(P\vee Q)\Leftrightarrow P$	
E_{10}	$\neg(P\vee Q)\Leftrightarrow\neg P\wedge\neg Q$	德·摩根定律
E_{10}'	$\neg(P\wedge Q)\Leftrightarrow\neg P\vee\neg Q$	

我们知道，一个命题公式是由命题变元、联结词和圆括号所组成的符号串。如果 C 是公式 A 的一部分（即 C 是公式 A 中连续的几个符号），而 C 本身也是一个公式，则称 C 为公式 A 的**子公式**。例如，设公式 A 为

$$(P\vee Q)\to(Q\vee(R\wedge P)),$$

则 $(P\vee Q)$、$(R\wedge P)$、$(Q\vee(R\wedge P))$ 都是A的子公式。而 $(P\vee Q)\rightarrow$、$(Q\vee(R\wedge$、$(R\wedge P))$ 都不是A的子公式。因为它们本身不是公式。

下面我们介绍置换规则和代入规则。

置换规则：设C是公式A的一个子公式，$C\Leftrightarrow D$。如果将公式A中的子公式C置换成公式D之后，得到的公式是B，则$A\Leftrightarrow B$。

证明 设$P_1, P_2, \cdots, P_n$是公式A和公式B中出现的全部命题变元。因为C和D分别是A和B的子公式，所以C和D中所出现的命题变元都包含在$P_1, P_2, \cdots, P_n$之中。由于$C\Leftrightarrow D$，因此对于命题变元$P_1, P_2, \cdots, P_n$的任意一组指派，C与D的取值均相同，于是A与B的取值也必然相同。按照公式等值的定义，有$A\Leftrightarrow B$。证完。

由于等值关系具有传递性，因此，公式A按照置换规则进行任意多次置换后，所得到的公式仍与公式A等值。

代入规则：对于重言式中的任一命题变元出现的每一处均用同一命题公式代入，得到的仍是重言式。

由于重言式的值不依赖于命题变元值的变化，因此，对命题变元按照代入规则作代入后，并不影响此重言式，故代入规则是正确的。

于是，若对于等值式中的任一命题变元出现的每一处均用同一命题公式代入，则仍得到等值式。因此，表 9-1 所列出的 19 个等值式，不仅对于任意的命题变元P, Q, R是成立的，而且当P, Q, R分别为某些命题公式时，这些等值式也仍然是成立的。所以，表 9-1 可以看成是 19 个等值模式。

有了置换规则和代入规则，我们便可以利用已知的一些公式等值式（如表 9-1 中的等值式）推导出其它一些更复杂的公式等值式。

例 2 证明 $(P\wedge(Q\wedge S))\vee(\neg P\wedge(Q\wedge S))\Leftrightarrow Q\wedge S$.

证明 $(P\wedge(Q\wedge S))\vee(\neg P\wedge(Q\wedge S))$

$\Leftrightarrow((Q\wedge S)\wedge P)\vee((Q\wedge S)\wedge\neg P)$ 由 E_1'

$\Leftrightarrow(Q\wedge S)\wedge(P\vee\neg P)$ 由 E_3

$\Leftrightarrow(Q\wedge S)\wedge 1$ 由 E_5

$\Leftrightarrow Q\wedge S$ 由 E_4'

例 3 证明 $Q\vee\neg((\neg P\vee Q)\wedge P)$ 是一个重言式.

证明 $Q\vee\neg((\neg P\vee Q)\wedge P)$

$\Leftrightarrow Q\vee(\neg(\neg P\vee Q)\vee\neg P)$ 由 E_{10}'

$\Leftrightarrow Q\vee((P\wedge\neg Q)\vee\neg P)$ 由 E_{10}

$\Leftrightarrow Q\vee((P\vee\neg P)\wedge(\neg Q\vee\neg P))$ 由 E_1, E_3'

$\Leftrightarrow Q\vee(1\wedge(\neg Q\vee\neg P))$ 由 E_5

$\Leftrightarrow Q\vee(\neg Q\vee\neg P)$ 由 E_1', E_4'

$\Leftrightarrow(Q\vee\neg Q)\vee\neg P$ 由 E_2

$\Leftrightarrow 1\vee\neg P$ 由 E_5

$\Leftrightarrow 1$ 由 E_1, E_8

因为公式 $Q\vee\neg((\neg P\vee Q)\wedge P)$ 与重言式等值，所以公式 $Q\vee\neg((\neg P\vee Q)\wedge P)$ 是重言式.

在表 9-1 中，我们没有列出任何一个包含联结词→和↔的公式之间的等值关系，这是因为在公式中这两个联结词可以用联结词¬，∧和∨来代替．即

$P\rightarrow Q\Leftrightarrow\neg P\vee Q$, $\quad E_{11}$

$P\leftrightarrow Q\Leftrightarrow(P\wedge Q)\vee(\neg P\wedge\neg Q)$. $\quad E_{12}$

等值式 E_{11} 在 §9.1 中已用真值表证明了，用同样的方法可以证明等值式 E_{12}. 从这个意义上来说，¬、∧和∨是三种基本的联结词。实际上，由德·摩根定律，我们有

$$P\wedge Q\Leftrightarrow\neg(\neg P\vee\neg Q),\quad P\vee Q\Leftrightarrow\neg(\neg P\wedge\neg Q).$$

这说明得到一个与给定公式等值，而且消除了$\wedge$的公式也是可能的。同样，在公式中消除$\vee$也是可能的。因此，联结词集合{$\neg$，$\vee$}和{$\neg$，$\wedge$}都是功能完备的。但是，一般情况下为了不至于因联结词的数目减少而使得公式的形式变得复杂，我们仍常采用五个联结词。

利用E_{11}和E_{12}我们可以证明任何包含有$\rightarrow$和$\leftrightarrow$的公式等值式。

例 4 证明 $P\rightarrow(Q\rightarrow R)\Leftrightarrow(P\wedge Q)\rightarrow R$ $\qquad E_{13}$

证明 $P\rightarrow(Q\rightarrow R)\Leftrightarrow\neg P\vee(\neg Q\vee R)$ 由 E_{11}

$\Leftrightarrow(\neg P\vee\neg Q)\vee R$ 由 E_2

$\Leftrightarrow\neg(P\wedge Q)\vee R$ 由 E_{10}'

$\Leftrightarrow(P\wedge Q)\rightarrow R$ 由 E_{11}

例 5 证明 $P\leftrightarrow Q\Leftrightarrow(P\rightarrow Q)\wedge(Q\rightarrow P)$ $\qquad E_{14}$

证明 $(P\rightarrow Q)\wedge(Q\rightarrow P)\Leftrightarrow(\neg P\vee Q)\wedge(\neg Q\vee P)$ 由 E_{11}

$\Leftrightarrow(\neg P\wedge\neg Q)\vee(\neg P\wedge P)\vee(Q\wedge\neg Q)\vee(Q\wedge P)$ 由 E_3

$\Leftrightarrow(P\wedge Q)\vee(\neg P\wedge\neg Q)\vee 0\vee 0$ 由 E_1, E_5'

$\Leftrightarrow(P\wedge Q)\vee(\neg P\wedge\neg Q)$ 由 E_4

$\Leftrightarrow P\leftrightarrow Q$ 由 E_{12}

公式之间的另一个重要关系是蕴含关系。

设A、B是两个公式，若公式$A\rightarrow B$是重言式，即$A\rightarrow B\Leftrightarrow 1$，则称**公式$A$蕴含公式$B$**，表示为$A\Rightarrow B$，这里符号“$\Rightarrow$”和“$\rightarrow$”的区别和联系与符号“$\Leftrightarrow$”和“$\leftrightarrow$”的区别和联系是完全类似的。

蕴含关系不满足对称性，即若$A\Rightarrow B$，则不一定有$B\Rightarrow A$成立，但它有以下几条性质：

(1) 自反性：对任意的公式A，$A\Rightarrow A$。

(2) 反对称性：对任意的公式A、B，若$A\Rightarrow B$，$B\Rightarrow A$，则$A\Leftrightarrow B$。

(3) 可传递性：对任意的公式 A、B、C，若 $A \Rightarrow B$，$B \Rightarrow C$，则 $A \Rightarrow C$。

这些性质都可以由定义直接证明。以可传递性为例，如果 $A \Rightarrow B$，$B \Rightarrow C$，那么按照定义，公式 $A \to B$ 和 $B \to C$ 都为重言式，即

$$\neg A \vee B \Leftrightarrow \neg B \vee C \Leftrightarrow 1$$

因此
$$\begin{aligned}
\neg A \vee C &\Leftrightarrow (\neg A \vee C) \vee 0 \\
&\Leftrightarrow (\neg A \vee C) \vee (B \wedge \neg B) \\
&\Leftrightarrow (\neg A \vee B \vee C) \wedge (\neg A \vee \neg B \vee C) \\
&\Leftrightarrow (1 \vee C) \wedge (\neg A \vee 1) \\
&\Leftrightarrow 1 \wedge 1 \\
&\Leftrightarrow 1
\end{aligned}$$

由于 $A \to C$ 为重言式，因此 $A \Rightarrow C$。

表 9-2 中列出了一些重要的蕴含关系。这些蕴含关系均可以按照定义直接证明，下面以[12]式为例给出其证明：

$$\begin{aligned}
&((P \to Q) \wedge (Q \to R)) \to (P \to R) \\
\Leftrightarrow &((\neg P \vee Q) \wedge (\neg Q \vee R)) \to (\neg P \vee R) \\
\Leftrightarrow &\neg((\neg P \vee Q) \wedge (\neg Q \vee R)) \vee (\neg P \vee R) \\
\Leftrightarrow &((P \wedge \neg Q) \vee (Q \wedge \neg R)) \vee (\neg P \vee R) \\
\Leftrightarrow &(P \wedge \neg Q) \vee ((Q \wedge \neg R) \vee (\neg P \vee R)) \\
\Leftrightarrow &(P \wedge \neg Q) \vee ((Q \vee \neg P \vee R) \wedge (\neg R \vee \neg P \vee R)) \\
\Leftrightarrow &(P \wedge \neg Q) \vee ((Q \vee \neg P \vee R) \wedge 1) \\
\Leftrightarrow &(P \wedge \neg Q) \vee (Q \vee \neg P \vee R) \\
\Leftrightarrow &(P \vee Q \vee \neg P \vee R) \wedge (\neg Q \vee Q \vee \neg P \vee R) \\
\Leftrightarrow &1 \wedge 1 \\
\Leftrightarrow &1
\end{aligned}$$

因此
$$((P \to Q) \wedge (Q \to R)) \Rightarrow P \to R$$

表 9-2

编号	蕴含关系式
[1]	$P\wedge Q\Rightarrow P$
[2]	$P\wedge Q\Rightarrow Q$
[3]	$P\Rightarrow P\vee Q$
[4]	$Q\Rightarrow P\vee Q$
[5]	$\neg P\Rightarrow P\to Q$
[6]	$Q\Rightarrow P\to Q$
[7]	$\neg(P\to Q)\Rightarrow P$
[8]	$\neg(P\to Q)\Rightarrow\neg Q$
[9]	$P\wedge(P\to Q)\Rightarrow Q$
[10]	$\neg Q\wedge(P\to Q)\Rightarrow\neg P$
[11]	$\neg P\wedge(P\vee Q)\Rightarrow Q$
[12]	$(P\to Q)\wedge(Q\to R)\Rightarrow P\to R$
[13]	$(P\vee Q)\wedge(P\to R)\wedge(Q\to R)\Rightarrow R$

为了证明给定的蕴含关系，可以假定相应的蕴含式命题的前件为真，检查在此情况下，其后件是否也为真，如果后件也为真，则说明此蕴含式命题公式是重言式，因而也就证明了该蕴含关系成立。例如在蕴含关系式[11]中，若假定$\neg P\wedge(P\vee Q)$的值为真，则$\neg P$和$P\vee Q$的值皆为真，于是P的值为假，从而Q的值为真。因此蕴含关系式[11]成立。

证明蕴含关系的另一种方法是，假定其后件为假，检查在此情况下，其前件是否有可能为真，如果前件不可能为真，则该蕴含关系成立。例如在蕴含关系式[10]中，假定$\neg P$的值为假，则P的值为真。若Q的值为真，则$\neg Q$的值为假，从而$\neg Q\wedge(P\to Q)$的值为假；若Q的值为假，则$P\to Q$的值为假，也得到$\neg Q\triangle(P\to Q)$的值为假，因此说明蕴含关系式[10]成立。

显然，若$A\Rightarrow B$且$A\Rightarrow C$，则$A\Rightarrow(B\triangle C)$。

如果一个重言式蕴含某个公式，那么这个公式一定也是重言

式。因此，利用公式的这种蕴含关系，我们可以证明某些公式为重言式。

例 5 中我们证明了公式 $P \leftrightarrow Q$ 与公式 $(P \rightarrow Q) \wedge (Q \rightarrow P)$ 是两个等值的公式。这说明对于任意的两个公式 P 和 Q，所谓 P 和 Q 等值即意味着 P 蕴含 Q 且 Q 蕴含 P。

我们知道，一个公式 A 如果包含有联结词 $\rightarrow$ 和 $\leftrightarrow$，则可以用前面的 E_{11} 和 E_{12} 经过置换化成一个与之等值的公式 B，而公式 B 只包含三种基本联结词 $\neg$、$\wedge$ 和 $\vee$。因此在下面关于对偶原理的讨论中，我们可以假定每个公式中只出现 $\neg$、$\wedge$ 和 $\vee$ 这三种联结词。

我们定义联结词 $\neg$、$\wedge$ 和 $\vee$ 的对偶分别是联结词 $\neg$、$\vee$ 和 $\wedge$。对偶用 D 表示，即

$$\wedge^D = \vee, \quad \vee^D = \vee, \quad \neg^D = \neg.$$

又定义　　$1^D = 0$，$0^D = 1$。

设 $A(P_1, P_2, \cdots, P_n)$ 是一个命题公式，其中 $P_1, P_2, \cdots, P_n$ 是公式中所包含的命题变元，如果将此公式中的基本联结词及 1 和 0 分别改为它们的对偶，其它符号均保持不变，则这样得到的公式称为是原公式 A 的对偶。表示成 $A^D(P_1, P_2, \cdots, P_n)$。显然，$A$ 和 A^D 互为对偶。

例如，公式 $((P \vee \neg Q) \wedge R) \vee (S \wedge P)$ 与公式 $((P \wedge \neg Q) \vee R) \wedge (S \vee P)$ 互为对偶。

定理 9-1　设 A 和 A^D 是互为对偶的两个公式，$P_1, P_2, \cdots, P_n$ 是其命题变元，则

$$\neg A(P_1, P_2, \cdots, P_n) \Leftrightarrow A^D(\neg P_1, \neg P_2, \cdots, \neg P_n) \qquad (*)$$

证明　令 $A(P_1, P_2, \cdots, P_n)$ 中包含的 $\neg$、$\wedge$ 和 $\vee$ 的数目 l 为该公式的逻辑高度。施归纳于高度。

当 $l = 0$ 时，$(*)$ 式显然成立。

当 $l = 1$ 时，A 为以下三种情形之一：$A = P_1 \vee P_2$，$A = P_1 \wedge P_2$

或 $A=\neg P$。

(1) 若 $A=P_1\vee P_2$，则 $A^D=P_1\wedge P_2$。由德·摩根定律

$$\neg(P_1\vee P_2)\Leftrightarrow\neg P_1\wedge\neg P_2.$$

(2) 若 $A=P_1\wedge P_2$，则 $A^D=P_1\vee P_2$。由德·摩根定律

$$\neg(P_1\wedge P_2)\Leftrightarrow\neg P_1\vee\neg P_2.$$

(3) 若 $A=\neg P$，则 $A^D=\neg P$。显然 $\neg(\neg P)\Leftrightarrow\neg(\neg P)$。

由此证明了当 $l=1$ 时，(*)式成立。

设(*)式在 $l\leqslant k-1$ 时皆成立，则当 $l=k$ 时，(*)式的正确性可证明如下：

$A(P_1,P_2,\cdots,P_n)$ 的最后一个运算符号仅可能为 $\vee$、$\wedge$ 或 $\neg$。

(1) 若最后一个运算符为 $\vee$，令

$$A(P_1,P_2,\cdots,P_n)=A_1(P_1,P_2,\cdots,P_n)\vee A_2(P_1,P_2,\cdots,P_n),$$

则 $l(A_1)$，$l(A_2)\leqslant k-1$，由归纳假设

$$\neg A_1(P_1,P_2,\cdots,P_n)\Leftrightarrow A_1^D(\neg P_1,\neg P_2,\cdots,\neg P_n),$$

$$\neg A_2(P_1,P_2,\cdots,P_n)\Leftrightarrow A_2^D(\neg P_1,\neg P_2,\cdots,\neg P_n).$$

因此
$$\begin{aligned}A^D(\neg P_1,\neg P_2,\cdots,\neg P_n)&=(A_1(\neg P_1,\neg P_2,\cdots,\neg P_n)\vee\\&\quad A_2(\neg P_1,\neg P_2,\cdots,\neg P_n))^D\\&\Leftrightarrow A_1^D(\neg P_1,\neg P_2,\cdots,\neg P_n)\wedge A_2^D(\neg P_1,\neg P_2,\cdots,\neg P_n)\\&\Leftrightarrow\neg A_1(P_1,P_2,\cdots,P_n)\wedge\neg A_2(P_1,P_2,\cdots,P_n)\\&\Leftrightarrow\neg(A_1(P_1,P_2,\cdots,P_n)\vee A_2(P_1,P_2,\cdots,P_n))\\&\Leftrightarrow\neg A(P_1,P_2,\cdots,P_n).\end{aligned}$$

由对称性 $\neg A(P_1,P_2,\cdots,P_n)\Leftrightarrow A^D(\neg P_1,\neg P_2,\cdots,\neg P_n)$。

(2) 若最后一个运算符为 $\wedge$，可类似于(1)地证明。

(3) 若最后一个运算符为 $\neg$，令

$$A(P_1,P_2,\cdots,P_n)=\neg A_1(P_1,P_2,\cdots,P_n),$$

则 $l(A_1)=k-1$，由归纳假设

$$\neg A_1(P_1,P_2,\cdots,P_n)\Leftrightarrow A_1^D(\neg P_1,\neg P_2,\cdots,\neg P_n).$$

因此 $\neg A(P_1,P_2,\cdots,P_n)=\neg(\neg A_1(P_1,P_2,\cdots,P_n))$

$$\Leftrightarrow \neg A_1^D(\neg P_1,\neg P_2,\cdots,\neg P_n)$$
$$\Leftrightarrow (\neg A_1(\neg P_1,\neg P_2,\cdots,\neg P_n))^D$$
$$\Leftrightarrow A^D(\neg P_1,\neg P_2,\cdots,\neg P_n).$$

由此证明了当 $l=k$ 时，(*)式成立。证完。

定理 9-2 （对偶原理）

设 $A(P_1, P_2, \cdots, P_n)$ 和 $B(P_1, P_2, \cdots, P_n)$ 是两个公式，若 $A\Leftrightarrow B$，则 $A^D\Leftrightarrow B^D$。

证明 因为 $A(P_1,P_2,\cdots,P_n)\Leftrightarrow B(P_1,P_2,\cdots,P_n)$，

所以 $\neg A(P_1,P_2,\cdots,P_n)\Leftrightarrow \neg B(P_1,P_2,\cdots,P_n)$。

由定理 9-1 $\neg A(P_1,P_2,\cdots,P_n)\Leftrightarrow A^D(\neg P_1,\neg P_2,\cdots,\neg P_n)$，

$\neg B(P_1,P_2,\cdots,P_n)\Leftrightarrow B^D(\neg P_1,\neg P_2,\cdots,\neg P_n)$。

于是 $A^D(\neg P_1,\neg P_2,\cdots,\neg P_n)\Leftrightarrow B^D(\neg P_1,\neg P_2,\cdots,\neg P_n)$。

从而 $A^D(P_1,P_2,\cdots,P_n)\Leftrightarrow B^D(P_1,P_2,\cdots,P_n)$。证完。

表 9-1 中每两个等值关系式 E_i 和 E_i' 都是互为对偶的，因此由对偶原理，我们只要证明其中的一个。

考虑所有命题的集合 S。显然，前面所定义的三种运算 $\neg$、$\wedge$和$\vee$分别可以看作是该集合上的一元和二元运算。因此，这个集合和这三个运算构成一个代数系统 $\langle S;\neg,\vee,\wedge\rangle$。由于这些运算满足交换律、分配律、同一律和互否律，因此，与集合代数 $\langle 2^U;',\cup,\cap\rangle$一样，代数系统$\langle S;\neg,\vee,\wedge\rangle$也是一个布尔代数，我们称它为命题代数。

§9.3 范 式

判断一个命题公式是否为重言式，或者矛盾式，或者是可满足的公式，这样的问题称作一个判定问题。在命题逻辑中，对于含有有限个命题变元的命题公式来说，用真值表的方法，总可以

在有限的步骤内确定它的真值。因此判定问题总是可解的。但是正如前面曾指出过的，这种方法并不理想。因为当命题变元较多时，运算次数很大，每增加一个命题变元，真值表的行数就增加一倍。本节给出对公式进行判定的另一种方法，为此我们先引进几个概念。

质合取式：一个由命题变元或命题变元的否定所组成的合取式称为质合取式。

质析取式：一个由命题变元或命题变元的否定所组成的析取式称为质析取式。

例如，设 P 和 Q 是两个命题变元，那么 P、$P\wedge Q$、$\neg P\wedge Q\wedge P$ 等都是质合取式，而 P、$P\vee Q$、$\neg P\vee P\vee Q$、$P\vee\neg Q$ 等都是质析取式。

定理 9-3

(1) 一质合取式为矛盾式的充分必要条件是：它同时包含某个命题变元 P 及其否定 $\neg P$。

(2) 一质析取式为重言式的充分必要条件是：它同时包含某个命题变元 P 及其否定 $\neg P$。

证明 (1) 充分性：对于任何命题变元 P，$P\wedge\neg P$ 是矛盾式，因此，若有 $P\wedge\neg P$ 在质合取式中出现，则这个质合取式必为矛盾式。

必要性：假设一个质合取式为矛盾式，但式中不同时包含任一命题变元及其否定。那么，我们对该合取式中出现在否定号后面的命题变元指派值 0，而对不出现在否定号后面的命题变元指派值 1，则整个合取式取值必为 1，这与假设矛盾。证完。

(2) 的证明方法与(1)同。

析取范式：质合取式的析取称为析取范式。

合取范式：质析取式的合取称为合取范式。

例如 $(\neg P\wedge\neg Q)\vee(P\wedge Q)\vee(P\wedge R\wedge\neg Q)$，

$$(P\wedge Q\wedge \neg P)\vee(Q\wedge \neg Q)$$

等都是析取范式。

$$(\neg P\vee \neg Q)\wedge(P\vee \neg Q),$$
$$(P\vee Q\vee \neg Q)\wedge(P\vee \neg P)$$

等都是合取范式。

任一命题公式都可以变换为与它等值的析取范式和合取范式的形式。其步骤如下：

(1) 消去公式中的运算符 $\rightarrow$ 和 $\leftrightarrow$：利用 E_{11} 和 E_{12} 将公式中出现的 $P\rightarrow Q$ 置换为 $\neg P\vee Q$，$P\leftrightarrow Q$ 置换为 $(P\wedge Q)\vee(\neg P\wedge \neg Q)$ 或者 $(\neg P\vee Q)\wedge(\neg Q\vee P)$。

(2) 将否定号 $\neg$ 向内深入，使之只作用于命题变元：利用德·摩根定律将公式中出现的 $\neg(P\vee Q)$ 置换为 $\neg P\wedge \neg Q$。$\neg(P\wedge Q)$ 置换为 $\neg P\vee \neg Q$。

(3) 利用双重否定律将 $\neg(\neg P)$ 置换成 P。

(4) 利用分配律将公式变为所需要的范式：

将 $P\wedge(Q\vee R)$ 置换为 $(P\wedge Q)\vee(P\wedge R)$ 可得析取式。

将 $P\vee(Q\wedge R)$ 置换为 $(P\vee Q)\wedge(P\vee R)$ 可得合取式。

由于每一个命题公式都是有限长的符号序列，因此，经过有限次的置换以后，必可得到与原公式等值的范式。

例 1 求公式 $P\leftrightarrow(P\wedge Q)$ 的析取范式。

方法一：
$$\begin{aligned}P\leftrightarrow(P\wedge Q)&\Leftrightarrow(P\wedge P\wedge Q)\vee(\neg P\wedge \neg(P\wedge Q))\\&\Leftrightarrow(P\wedge P\wedge Q)\vee(\neg P\wedge(\neg P\vee \neg Q))\\&\Leftrightarrow(P\wedge P\wedge Q)\vee(\neg P\wedge \neg P)\\&\quad\vee(\neg P\wedge \neg Q).\end{aligned}$$

方法二：
$$\begin{aligned}P\leftrightarrow(P\wedge Q)&\Leftrightarrow(\neg P\vee(P\wedge Q))\wedge(\neg(P\wedge Q)\vee P)\\&\Leftrightarrow(\neg P\vee(P\vee Q))\wedge(\neg P\vee \neg Q\vee P)\\&\Leftrightarrow(\neg P\wedge(\neg P\vee \neg Q\vee P))\vee((P\wedge Q)\\&\quad\vee(\neg P\vee \neg Q\vee P))\end{aligned}$$

$$\Leftrightarrow(\neg P\wedge\neg P)\vee(\neg P\wedge\neg Q)\vee(\neg P\wedge P)\vee(P\wedge Q\wedge\neg P)\vee(P\wedge Q\wedge\neg Q)\vee(P\wedge Q\wedge P)$$

由上看出，一个公式的析取范式不是唯一的。然而同一公式的不同析取范式是等值的。

例 2 求公式 $P\wedge(P\rightarrow Q)$ 的合取范式。

解 $P\wedge(P\rightarrow Q)\Leftrightarrow P\wedge(\neg P\vee Q)$。

而
$$P\wedge(\neg P\vee Q)\Leftrightarrow(P\wedge\neg P)\vee(P\wedge Q)$$
$$\Leftrightarrow(P\vee P)\wedge(P\vee Q)\wedge(\neg P\vee P)\wedge(\neg P\vee Q)。$$

因此，一个公式的合取范式也不是唯一的。

定理 9.4

(1) 公式 A 为重言式的充分必要条件是：A 的合取范式中每一质析取式至少包含有一对互为否定的析取项。

(2) 公式 A 为矛盾式的充分必要条件是：A 的析取范式中每一质合取式至少包含一对互为否定的合取项。

证明留给读者。

例 3 判别公式 $\neg(P\vee R)\vee\neg(Q\wedge\neg R)\vee P$ 是否为重言式或矛盾式。

解 求其范式：
$$\neg(P\vee R)\vee\neg(Q\wedge\neg R)\vee P$$
$$\Leftrightarrow(\neg P\wedge\neg R)\vee\neg Q\vee R\vee P。$$

在公式的析取范式中，共有 4 个析取项，但任何一个中都没有同一命题变元及其否定同时出现。故原公式不是矛盾式。

应用$\vee$对$\wedge$的分配律
$$(\neg P\wedge\neg R)\vee\neg Q\vee R\vee P$$
$$\Leftrightarrow(\neg P\vee\neg Q\vee R\vee P)\wedge(\neg R\vee\neg Q\vee R\vee P)。$$

在公式的合取范式中，第一个合取项中同时包含有 $\neg P$ 和 P，第二个合取项中同时包含有 $\neg R$ 和 R，因此原公式为重言式。

例 4 判别公式 $(P\rightarrow Q)\rightarrow P$ 是否为重言式或矛盾式。

解 求其范式

$$
\begin{aligned}
(P\rightarrow Q)\rightarrow P &\Leftrightarrow (\neg P\vee Q)\rightarrow P\\
&\Leftrightarrow \neg(\neg P\vee Q)\vee P\\
&\Leftrightarrow (P\wedge\neg Q)\vee P.
\end{aligned}
$$

又
$$(P\wedge\neg Q)\vee P\Leftrightarrow(P\vee P)\wedge(\neg Q\vee P).$$

由于公式 $(P\rightarrow Q)\rightarrow P$ 的析取范式和合取范式均不满足定理9-4的条件，因此它既不是矛盾式也不是重言式。它是一个可满足的公式。事实上，若令 P 的值为 1，则 $(P\rightarrow Q)\rightarrow P$ 的值为 1.

利用合取范式和析取范式虽然可以较容易地判别一个公式是否为重言式或矛盾式，但它们有不足之处，那就是一个公式的合取范式和析取范式不是唯一的。这对于希望通过范式来判别两公式是否等值带来了不便。为了使各公式的范式能够是唯一的，我们进一步介绍主范式的概念。

设有命题变元 $P_1, P_2, \cdots, P_n$，形如 $\bigwedge_{i=1}^{n} P_i^*$ 的命题公式称为是由命题变元 $P_1, P_2, \cdots, P_n$ 所产生的**最小项**。而形如 $\bigvee_{i=1}^{n} P_i^*$ 的命题公式称为是由命题变元 $P_1, P_2, \cdots, P_n$ 所产生的**最大项**。其中每一个 P_i^* 或为 P_i 或为 $\neg P_i$。

显然，最小项和最大项分别是一些特殊的质合取式和质析取式，且由 $P_1, P_2, \cdots, P_n$ 产生的不同最小项和不同最大项分别为 2^n 个。将集合 $A_1, A_2, \cdots, A_n$ 分别换成命题变元 $P_1, P_2, \cdots, P_n$，A_i' 换成 $\neg P_i$，$\cup$ 换成 $\vee$，$\cap$ 换成 $\wedge$，作类似于 §1.9 的讨论，可得到与集合代数中完全类似的结论。

例如，我们作三个命题变元 P_1，P_2，P_3 所产生的某些最小项的真值表

P_1	P_2	P_3	$\neg P_1\wedge\neg P_2\wedge P_3$	$\neg P_1\wedge P_2\wedge P_3$	$P_1\wedge P_2\wedge\neg P_3$	$P_1\wedge P_2\wedge P_3$
0	0	0	0	0	0	0
0	0	1	1	0	0	0
0	1	0	0	0	0	0
0	1	1	0	1	0	0
1	0	0	0	0	0	0
1	0	1	0	0	0	0
1	1	0	0	0	1	0
1	1	1	0	0	0	1

由表中可以看出，对于每一个最小项$\bigwedge_{i=1}^{n}P_i^*$，仅有表中的一行使其值为1，该行就是$P_1^*,P_2^*,\cdots,P_n^*$所标记的列分别为1的行，也就是$P_1,P_2,\cdots,P_n$所标记的各列分别为$\delta_1,\delta_2,\cdots,\delta_n$的行，其中

$$\delta_i=\begin{cases}0 & 当\ P_i^*=\neg P_i\\ 1 & 当\ P_i^*=P_i\ .\end{cases}$$

于是，不同的最小项取值为1的行各不相同，而每一行都必有一最小项在该行取值为1．因此，对于任一给定的公式A，作出它的真值表，根据它在真值表中取值为1的个数和1所在的行，可作出一个与A等值且由若干个不同最小项的析取所构成的公式．该公式中不同最小项的个数等于A在真值表中1的个数，而这些最小项在真值表中取值为1的行分别对应着A的取值为1的不同的行．于是，类似于定理1-4我们有：

定理9-5 每一个不为矛盾式的命题公式$A(P_1,P_2,\cdots,P_n)$必与一个由$P_1,P_2,\cdots,P_n$所产生的不同最小项的析取式等值．

这种由不同最小项所组成的析取式，我们称它为**主析取范式**．每一个不为矛盾式的公式都有一个与之等值的主析取范式．对于矛盾式$A(P_1,P_2,\cdots,P_n)$，由于它的主析取范式不能包含2^n个最小项中的任何一个，因此我们说，矛盾式的主析取范式是空公式，

定义它为 0。若公式 $A(P_1,P_2,\cdots,P_n)$ 是重言式，那么所有 2^n 个最小项都会出现在它的主析取范式中。因此，利用一个公式的主析取范式可以判别这个公式是否为重言式或矛盾式。

类似地，对于每一个最大项 $\bigvee_{i=1}^{n} P_i^*$，仅有真值表中的一行使其值为 0。该行就是 $P_1, P_2, \cdots, P_n$ 所标记的各列分别为 $\delta_1,\delta_2,\cdots,\delta_n$ 的行。其中

$$\delta_i=\begin{cases}0 & \text{当 } P_i^*=P_i\\ 1 & \text{当 } P_i^*=\neg P_i\text{。}\end{cases}$$

不同的最大项取值为 0 的行各不相同，而每一行都必有一最大项在该行取值为 0。因此，对于任一给定的公式 A，作出它的真值表，根据它在真值表中取值为 0 的个数和 0 所在的行，可作出一个与 A 等值且由若干个不同最大项的合取所构成的公式，这些不同最大项的个数等于 A 在真值表中 0 的个数，而这些最大项在真值表中取值为 0 的行分别对应着 A 的取值为 0 的不同的行。于是类似于定理 1-5，我们有

定理 9-6 每一个不是重言式的公式 $A(P_1,P_2,\cdots,P_n)$ 必与一个由 $P_1,P_2,\cdots,P_n$ 所产生的不同最大项的合取式等值。

这种由不同最大项所组成的合取式称为**主合取范式**。每一个不为重言式的公式都有一个与之等值的主合取范式。与主析取范式相反，重言式的主合取范式是空公式，定义它为 1。矛盾式的主合取范式必由所有最大项的合取构成。因此，利用一个公式的主合取范式也可判别这个公式是否为重言式或矛盾式。

求一个给定公式的主析取范式和主合取范式不一定要借助于真值表，用类似于求范式的方法也可求出给定公式的主范式。不过在求公式的主范式时，除了使用求范式时的四个步骤外，还要作以下三项置换：

(5) 利用同一律消去矛盾的质合取式（重言的质析取式）。

(6) 利用等幂律消去相同的质合取式（质析取式）、消去质合取式（质析取式）中相同的合取项（析取项）。

(7) 利用同一律、分配律将不包含某一命题变元的质合取式（质析取式）置换为包含有这一命题变元的质合取式（质析取式）。

把$(P\wedge Q)$置换为$(P\wedge Q)\wedge(R\vee\neg R)$，再置换为$(P\wedge Q\wedge R)\vee(P\wedge Q\wedge\neg R)$。

把$(P\vee Q)$置换为$(P\vee Q)\vee(R\wedge\neg R)$，再置换为$(P\vee Q\vee R)\wedge(P\vee Q\vee\neg R)$。

例 5 给定公式$(P\wedge(P\to Q))\to Q$，求其主范式并对公式是否重言式或矛盾式进行判定。

解 求公式的主析取范式

$$
\begin{aligned}
&(P\wedge(P\to Q))\to Q\\
&\Leftrightarrow\neg(P\wedge(\neg P\vee Q))\vee Q\\
&\Leftrightarrow\neg P\vee\neg(\neg P\vee Q)\vee Q\\
&\Leftrightarrow\neg P\vee(P\wedge\neg Q)\vee Q\\
&\Leftrightarrow(\neg P\wedge(Q\vee\neg Q))\vee(P\wedge\neg Q)\vee(Q\wedge(P\vee\neg P))\\
&\Leftrightarrow(\neg P\wedge Q)\vee(\neg P\wedge\neg Q)\vee(P\wedge\neg Q)\vee(P\wedge Q)\vee(\neg P\wedge Q)\\
&\Leftrightarrow(P\wedge Q)\vee(\neg P\wedge Q)\vee(P\wedge\neg Q)\vee(\neg P\wedge\neg Q)。
\end{aligned}
$$

由于公式的主析取范式包含了所有的最小项，因此原公式为重言式。

原公式为重言式的结论也可通过求主合取范式而得到。

$$
\begin{aligned}
(P\wedge(P\to Q))\to Q&\Leftrightarrow\neg P\vee(P\wedge\neg Q)\vee Q\\
&\Leftrightarrow((\neg P\vee P)\wedge(\neg P\vee\neg Q))\vee Q\\
&\Leftrightarrow(\neg P\vee\neg Q)\vee Q\\
&\Leftrightarrow\neg P\vee\neg Q\vee Q\Leftrightarrow 1
\end{aligned}
$$

由于仅有的质析取式是一重言式，消去后所得的主合取范式是一空公式，因此原公式是重言式。

例 6 求公式$(\neg P\to R)\wedge(P\leftrightarrow Q)$的主合取范式和主析取范

式。

解　将公式 $(\neg P\rightarrow R)\wedge(P\leftrightarrow Q)$ 简记成 S。

$$S\Leftrightarrow(P\vee R)\wedge(\neg P\vee Q)\wedge(\neg Q\vee P)$$

$$\Leftrightarrow(P\vee R\vee(Q\wedge\neg Q))\wedge(\neg P\vee Q\vee(R\wedge\neg R))\wedge(P\vee\neg Q\vee(R\wedge\neg R))$$

$$\Leftrightarrow(P\vee Q\vee R)\wedge(P\vee\neg Q\vee R)\wedge(\neg P\vee Q\vee R)\wedge(\neg P\vee Q\vee\neg R)\wedge(P\vee\neg Q\vee R)\wedge(P\vee\neg Q\vee\neg R)$$

$$\Leftrightarrow(P\vee Q\vee R)\wedge(P\vee\neg Q\vee R)\wedge(P\vee\neg Q\vee\neg R)\wedge(\neg P\vee Q\vee R)\wedge(\neg P\vee Q\vee\neg R).$$

此即 S 的主合取范式。

显然，余下的最大项的合取式便是 $\neg S$ 的主合取范式。即

$$\neg S\Leftrightarrow(P\vee Q\vee\neg R)\wedge(\neg P\vee\neg Q\vee R)\wedge(\neg P\vee\neg Q\vee\neg R).$$

对 $\neg S$ 求否定，并利用定理 9-1，便得到 S 的主析取范式

$$S\Leftrightarrow\neg(\neg S)$$

$$\Leftrightarrow(\neg P\wedge\neg Q\wedge R)\vee(P\wedge Q\wedge\neg R)\vee(P\wedge Q\wedge R).$$

由上看出，公式 S 既不是重言式也不是矛盾式，因而是一个可满足的公式。

类似于定理 1-6，我们有

定理 9-7　设 A 是包含命题变元 $P_1, P_2, \cdots, P_n$ 的命题公式，若不计其中最小项（最大项）的排列次序，则 A 的主析取范式(主合取范式)是唯一的。

利用公式的真值表，很容易得出定理的结论。

于是，两个公式等值的充分必要条件是它们的主析取范式(主合取范式）相同。

例如，下面的两个公式：

$$(\neg P\vee Q)\wedge(\neg Q\vee R)\wedge(\neg R\vee P)$$

和

$$(\neg Q\vee P)\wedge(\neg R\vee Q)\wedge(\neg P\vee R),$$

它们是不同的合取范式，但它们有相同的主合取范式：

$$(P\vee Q\vee \neg R)\wedge(P\vee \neg Q\vee R)\wedge(\neg P\vee Q\vee R)\wedge(P\vee \neg Q\vee \neg R)\wedge(\neg P\vee Q\vee \neg R)\wedge(\neg P\vee \neg Q\vee R)。$$

因此，这两个公式是等值的。

§9.4 命题演算的推理理论

推理是由已知的命题得到新命题的思维过程。任何一个推理都由前提和结论两部分组成，前提就是推理所根据的已知的命题，结论则是从前提通过推理而得到的新命题。

设 A 和 B 是两个命题公式，如果 $A\Rightarrow B$，即如果命题公式 $A\rightarrow B$ 为重言式，则我们说"从 A 推出 B"或说"B 是前提 A 的结论"。一般地，设 $H_1,H_2,\cdots,H_n$ 和 C 是一些命题公式，如果

$$H_1\wedge H_2\wedge\cdots\wedge H_n\Rightarrow C,$$

则称从前提 $H_1,H_2,\cdots,H_n$ 推出结论 C。有时也记为 $H_1,H_2,\cdots,H_n\Rightarrow C$。

一组前提是否可以推出某个结论，可以按照定义进行判断。

例 1 确定结论 C 是否可以从前提 H_1 及 H_2 推出。

(1) H_1：$P\rightarrow Q$，H_2：P，C：Q

(2) H_1：$P\rightarrow Q$，H_2：Q，C：P

解 构造上述命题公式的真值表

P	Q	$P\rightarrow Q$	$(P\rightarrow Q)\wedge P$	$(P\rightarrow Q)\wedge Q$
0	0	1	0	0
0	1	1	0	1
1	0	0	0	0
1	1	1	1	1

对于 (1) 我们看到，第四行是两个前提的真值都取 1 的唯一的行，在这一行结论 Q 也具有真值 1. 因此，C 是前提 H_1 和 H_2 的结论。对于 (2) 我们注意到，第二行和第四行是两个前提的真值都取 1 的行，但对于第二行，结论 P 的真值为 0. 因此，$H_1 \wedge H_2 \rightarrow C$ 不是重言式. 按照定义，(2) 中的两个前提不能推出结论 C。

例如，将某些具体的命题代入命题变元 P 和 Q，根据 (1) 我们得到下述两个断言：

(1) 如果今天出太阳，他就进城，
今天出了太阳，
所以他进城了.

(2) 如果狗有翅膀，则狗会飞上天，
狗有翅膀，
所以狗飞上天了.

(3) 如果 n 是素数，则 n 一定是整数，
n 是整数，
所以 n 是素数.

显然(1)是正确的，(2)看起来似乎很荒唐。但是，由于数理逻辑主要是从抽象的逻辑关系上来研究推理，因此，在 (2) 中虽然前件和后件都是假的，但是这种推理形式却是正确的。(3) 的结论是错误的，错误在于命题公式 $((P \rightarrow Q) \wedge Q) \rightarrow P$ 不是重言式。这也就是我们在数学中常说到的"当乙是甲的必要条件时，乙不一定是甲的充分条件".

判断 $H_1 \wedge H_2 \wedge \cdots \wedge H_n \rightarrow C$ 是否为重言式，我们还可以仿照 §9.2 中的方法，利用已知的一些等值式推导出等值式 $(H_1 \wedge H_2 \wedge \cdots \wedge H_n \rightarrow C) \Leftrightarrow 1$，从而证明 C 是前提 $H_1, H_2, \cdots, H_n$ 的结论。

例 2 证明 C：$\neg P$ 是前提 H_1：$P \rightarrow Q$ 和 H_2：$\neg(P \wedge Q)$ 的结论。

证明 $H_1\wedge H_2\to C\Leftrightarrow((P\to Q)\wedge\neg(P\wedge Q))\to\neg P$

$$\Leftrightarrow((\neg P\vee Q)\wedge(\neg P\vee\neg Q))\to\neg P$$

$$\Leftrightarrow(\neg P\vee(Q\wedge\neg Q))\to\neg P$$

$$\Leftrightarrow\neg P\to\neg P$$

$$\Leftrightarrow P\vee\neg P$$

$$\Leftrightarrow 1$$

由定义可知，C 是前提 H_1 和 H_2 的结论。

上面两个例子基本上是按照定义来证明的，但当前提和结论都是比较复杂的命题公式或者所包含的命题变元很多的时候，直接用定义进行推导将是很困难的。因此需要寻求更有效的推理方法。

为了证明 C 是前提 H_1，H_2，…，H_n 的结论，我们需要证明 $(H_1\wedge H_2\wedge\cdots\wedge H_n)\to C$ 是一个重言式，也就是要证明当前提 H_1，H_2，…，H_n 均为真时，C 必为真。为了描述这样一个推理过程，我们可以构造一个命题序列，其中每个命题或者是已知的命题，或者是由某些前提所推得的结论，序列中最后一个命题就是所要求的结论。这样一个描述推理过程的命题序列称为是**形式证明**。要想进行正确的推理，就必须构造一个逻辑结构严谨的形式证明，这就需要使用一些推理规则。

下面几个规则是人们在推理过程中常用到的推理规则：

(1) **前提引入规则**：在证明的任何步骤上都可以引用前提。

(2) **结论引用规则**：在证明的任何步骤上所得到的结论都可以在其后的证明中引用。

(3) **置换规则**：在证明的任何步骤上，命题公式的子公式都可以用与之等值的其它命题公式置换。

(4) **代入规则**：在证明的任何步骤上，重言式中的任一命题变元都可以用一命题公式代入，得到的仍是重言式。

在§9.2中列出的 E_1—E_{14}，以及

E_{15} $\neg(P\to Q)\Leftrightarrow P\wedge\neg Q$

E_{16} $P\to Q\Leftrightarrow\neg Q\to\neg P$

E_{17} $\neg(P\leftrightarrow Q)\Leftrightarrow P\leftrightarrow\neg Q$

都是在推理过程中经常使用的一些等值关系式。

在推理过程中经常使用的蕴含关系式有：

I_1 $P\wedge Q\Rightarrow P$

I_2 $P\wedge Q\Rightarrow Q$

I_3 $P\Rightarrow P\vee Q$

I_4 $Q\Rightarrow P\vee Q$

I_5 $\neg P\Rightarrow P\to Q$

I_6 $Q\Rightarrow P\to Q$

I_7 $\neg(P\to Q)\Rightarrow P$

I_8 $\neg(P\to Q)\Rightarrow\neg Q$

I_9 P、$Q\Rightarrow P\wedge Q$

I_{10} $\neg P$、$P\vee Q\Rightarrow Q$

I_{11} P、$P\to Q\Rightarrow Q$

I_{12} $\neg Q$、$P\to Q\Rightarrow\neg P$

I_{13} $P\to Q$，$Q\to R\Rightarrow P\to R$

I_{14} $P\vee Q$，$P\to R$、$Q\to R\Rightarrow R$

这些蕴含式也被称为推理定律，因为它们给出了正确的推理形式。

蕴含关系式 I_{11} 称为假言推理，它表示：若两个命题为真，其中一个是蕴含式命题，而另一个是这个蕴含式命题的前件，那么这个蕴含式命题的后件一定也是真命题。在证明过程中，如果出现了某个推理定律的前件，则根据 I_{11}，立刻可得到由这个前件所推出的后件。因此，I_{11} 也被称为是**分离规则**。

如果证明过程中的每一步所得到的结论都是根据推理规则得到的，则这样的证明称作是**有效的**。通过有效的证明而得到的结论，称作是**有效的结论**。因此，一个证明是否有效与前提的真假

没有关系，一个结论是否有效与它自身的真假也没有关系。在数理逻辑中，主要关心的是如何构造一个有效的证明和得到有效的结论。如果所有的前提都是真的，那么通过有效的证明所得到的结论也是真的。这样的证明称作是**合理的**。通过合理的证明而得到的结论称作是**合理的结论**。数学中定理的证明过程一般都是一个合理的证明。

例 3 证明 $\neg P$ 是前提 $\neg(P\wedge\neg Q)$、$\neg Q\vee R$、$\neg R$ 的结论。

证明

编号	公式	依据
(1)	$\neg Q\vee R$	前提
(2)	$\neg R$	前提
(3)	$\neg Q$	(1),(2); I_{10}
(4)	$\neg(P\wedge\neg Q)$	前提
(5)	$\neg P\vee Q$	(4); E'_{10}, E_6
(6)	$\neg P$	(3),(5); I_{10}

表格中间一列是依次推导出来的命题公式，最后一行的命题公式 $\neg P$ 是要证明的结论。左边一列是推导出来的命题公式的编号，右边一列是推导的依据。

例 4 证明 $P\vee Q$ 是 $S\to Q$、$R\to P$、$S\vee R$ 的结论。

证明

编号	公式	依据
(1)	$S\vee R$	前提
(2)	$\neg S\to R$	(1); E_6, E_{11}
(3)	$R\to P$	前提
(4)	$\neg S\to P$	(2),(3); I_{13}
(5)	$\neg P\to S$	(4); E_{16}, E_6
(6)	$S\to Q$	前提
(7)	$\neg P\to Q$	(5),(6); I_{13}
(8)	$P\vee Q$	(7); E_{11}, E_6

例 5 证明 $(P\wedge Q)\rightarrow R$、$\neg R\vee S$、$\neg S\Rightarrow P\rightarrow\neg Q$。

由等值关系式 E_{13}：$P\rightarrow(Q\rightarrow R)\Leftrightarrow(P\wedge Q)\rightarrow R$，设 P 是一组前提的合取，Q 是任一公式，则等值关系式 E_{13} 说明，如果 Q 包括到前提集合中去作为添加的前提，并且 R 可以从 $P\wedge Q$ 推出，那么 $Q\rightarrow R$ 可以从这组前提 P 推出。因此，如果结论是 $Q\rightarrow R$ 的形式，通常就使用 E_{13} 将 Q 作为一个添加的前提而证明 R 能从所给的前提和 Q 中推出。我们用这种方法来证明例 5。

证明

编 号	公 式	依 据
(1)	$\neg R\vee S$	前 提
(2)	$\neg S$	前 提
(3)	$\neg R$	(1),(2); I_{10}
(4)	$(P\wedge Q)\rightarrow R$	前 提
(5)	$\neg(P\wedge Q)$	(3),(4); I_{12}
(6)	$\neg P\vee\neg Q$	(5); E_{10}'
(7)	P	假 设
(8)	$\neg Q$	(6),(7); I_{10}, E_6

例 6 "如果电影已开演，那么大门关着；如果他们八点钟以前到达，那么大门开着；他们八点钟以前到达。所以，电影没有开演"。证明这些语句构成一个正确的推理。

令 P：电影已开演。

Q：大门关着。

R：他们八点钟以前到达。

我们只需证明从前提 $P\rightarrow Q$、$R\rightarrow\neg Q$、R 可以推出结论 $\neg P$（请读者自己完成这一证明）。

如果对于出现在公式 $H_1, H_2, \cdots, H_n$ 中的命题变元的任何一组真值指派，公式 $H_1, H_2, \cdots, H_n$ 中至少有一个为假，即它们的合取式 $H_1\wedge H_2\wedge\cdots\wedge H_n$ 是矛盾式，则称公式 $H_1, H_2, \cdots, H_n$ 是

不相容的。否则称公式 $H_1, H_2, \cdots, H_n$ **是相容的**。当且仅当存在着一个命题 R，使得

$$H_1 \wedge H_2 \wedge \cdots \wedge H_n \Rightarrow R \wedge \neg R$$

时，$H_1, H_2, \cdots, H_n$ 是不相容的。这里 R 是任一公式。

不相容的概念用在称为反证法或间接证明法的证明过程中。为了证明结论 C 可以从前提 $H_1, H_2, \cdots, H_n$ 推出，我们把 $\neg C$ 添加到这组前提中去，如果有某个公式 R 使得 $H_1 \wedge H_2 \wedge \cdots \wedge H_n \wedge \neg C \Rightarrow R \wedge \neg R$，则这组新的前提是不相容的。于是，当 $H_1 \wedge H_2 \wedge \cdots \wedge H_n$ 为真时，$\neg C$ 必为假，也就是当 $H_1 \wedge H_2 \wedge \cdots \wedge H_n$ 为真时，C 必为真。于是，C 可以由前提 $H_1, H_2, \cdots, H_n$ 推出。

例 7　证明 $P \rightarrow \neg Q$、$Q \vee \neg R$、$R \wedge \neg S \Rightarrow \neg P$

证明　用反证法。把 $\neg(\neg P)$ 作为添加的前提加入到前提的集合中去，证明由此导致矛盾。

编号	公式	依据
(1)	$\neg(\neg P)$	假设
(2)	P	(1);E_6
(3)	$P \rightarrow \neg Q$	前提
(4)	$\neg Q$	(2),(3);I_{11}
(5)	$Q \vee \neg R$	前提
(6)	$\neg R$	(4),(5);I_{10}
(7)	$R \wedge \neg S$	前提
(8)	R	(7);I_1
(9)	$R \wedge \neg R$	(6),(8);I_9

所以从前提 $P \rightarrow \neg Q$、$Q \vee \neg R$、$R \wedge \neg S$ 可以推出结论 $\neg P$。

（二）谓词演算

§9.5 谓词、个体词和量词

在命题演算里，我们把原子命题作为基本研究单位，对它不再进行分析，而研究由原子命题和联结词所组成的复合命题。研究复合命题的逻辑性质和复合命题间的逻辑关系等等。这样，有些推理形式命题逻辑就不能包括。例如

所有的人都是要死的。

张三是人，

所以张三是要死的。

从直观上看，第三个命题是前两个命题的结论。但是，从前面研究的命题推理理论却得不出来。因为它的前提和结论里都没有联结词，它们都是原子命题，用命题逻辑来表示，它的形式是 $P\wedge Q\rightarrow R$。显然，这不是命题逻辑里的重言式。造成上述缺陷的原因在于我们不能对原子命题作进一步的分析，从而显出前提和结论在形式结构方面的联系，因此我们就不可能认识到这种推理的形式和规律。

又如：李芳是大学生。

张岗是大学生。

由于它们是两个原子命题，只能用两个不同的符号来表示，但这样的符号不能揭示出这两个命题的共同特性。

在谓词演算中，我们通常将一个命题里表示思维对象的词称为**主词**或称**个体词**；将表示一个个体的性质或两个以及两个以上个体间的关系的词称为**谓词**。表示 n 个个体之间的关系的谓词称为 **n 元谓词**，表示一个个体的性质的谓词称为**一元谓词**。例如，

上例中“李芳”和“张岗”分别是个体词，“是大学生”是谓词。

我们用大写字母表示谓词，用小写字母表示个体或对象。例如，我们用 Q 表示谓词“是大学生”，用 a 和 b 分别表示“李芳”和“张岗”，则上面两个命题分别可以写成 $Q(a)$ 和 $Q(b)$。

在“a 比 b 大”、“a 位于 b 与 c 之间”这些命题里，a 和 b 或者 a、b 和 c 都代表一些个体，“……比……大”和“……位于……与……之间”是谓词。我们可以把它们分别表示成 $A(a, b)$ 和 $B(a, b, c)$。A 是二元谓词，B 是三元谓词。

一般地，一个由 n 个个体和 n 元谓词所组成的命题可表示为 $G(a_1, a_2, \cdots, a_n)$，其中 G 表示 n 元谓词，a_1，a_2，…，a_n 分别表示 n 个个体。a_1，a_2，…，a_n 的排列次序有时是重要的。例如，$B(a, b, c)$ 不能写为 $B(b, a, c)$，否则就成了命题“b 位于 a 与 c 之间”。

以前所引入的联结词，在这里仍然可以用来构成复合命题。例如，若我们用 $Q(a)$ 表示“李芳是大学生”，用 $G(b, c)$ 表示“张琦比小红高”，则命题“李芳是大学生且张琦比小红高”记成 $Q(a) \wedge G(b, c)$。“如果李芳是大学生，则张琦比小红高”记成 $Q(a) \rightarrow G(b, c)$。“李芳不是大学生”记成 $\neg Q(a)$。同样，使用联结词 $\vee$ 和 $\leftrightarrow$ 可分别用来形成下面的命题：$Q(a) \vee G(b, c)$、$Q(a) \leftrightarrow G(b, c)$。

个体词可以是**个体常元**或**个体变元**，当其为个体变元时，对于谓词 Q，$Q(x)$ 便是个体变元 x 的函数。即当给 x 代以不同的个体时，便得到不同的命题。这些命题都有相同的谓词。而对于谓词 A、B，$A(x, y)$ 和 $B(x, y, z)$ 分别是两个个体变元 x，y 和三个个体变元 x，y，z 的函数。我们称它们为**命题函数**。一般地，含有 n 个个体变元 x_1，x_2，…，x_n 的命题函数表示为 $P(x_1, x_2, \cdots, x_n)$。命题函数并不是一个命题，只有当其中所有的个体变元都分别代之以具体的个体后才表示一个命题。

个体变元所代表的对象的总体或个体变元取值的范围称为**个体域**. 个体域可以是有限集合也可以是无限集合.

下面我们来考虑这样一些命题:

1. 凡是球都是圆的.

2. 每一个苹果都是红的.

3. 任何一个有理数都等于某一分数.

这些命题可以改写成:

1. 对于所有的x, 如果x是球, 则x是圆的.

2. 对于所有的x, 如果x是苹果, 则x是红的.

3. 对于所有的x, 如果x是有理数, 则x等于某一分数.

我们把"对于所有的x"记成$\forall x$(或者(x)), 把谓词"是球"和"是圆的"分别记成A和B, 则上述命题1. 可表示成

$$\forall x(A(x)\to B(x))(\text{或者}(x)(A(x)\to B(x))).$$

类似地, 命题2. 和3. 也可以写成上述形式.

又如命题"如果x比y大, 则y不比x大". 若用A表示谓词"……比……大", 那么这个命题可以表示为

$$\forall x\forall y(A(x,y)\to \neg A(y,x)),$$

我们称符号$\forall x$(或(x))为**全称量词**. 全称量词用来表示"对所有的"、"对每一个"以及"对任意一个"等词句.

我们引入另外一种量词来表示"有某一个"、"至少存在一个"等词句. 如命题"有的自然数是素数"可以写成"至少存在一个x, x是自然数并且x是素数".

我们将"至少存在一个x"记成$\exists x$. 符号$\exists x$称为**存在量词**. 如果把谓词"是自然数"和"是素数"分别记成A和B, 那么这个命题可表示成

$$\exists x(A(x)\wedge B(x)).$$

§9.6 谓词演算公式

由 n 元谓词 P 和 n 个个体变元 x_1，x_2，…，x_n 构成的命题函数 $P(x_1, x_2, \cdots, x_n)$ 称为是谓词演算中的**原子公式**．一个命题或一个命题变元也称为谓词演算中的原子公式．

由原子公式出发，下面给出谓词演算中**公式**的递归定义：

1．每个原子谓词公式都是谓词公式．

2．如果 A 是谓词公式，则 $\neg A$ 也是谓词公式．

3．如果 A 和 B 是谓词公式，则 $(A\vee B)$、$(A\wedge B)$、$(A\rightarrow B)$、$(A\leftrightarrow B)$ 也是谓词公式．

4．如果 A 是谓词公式，x 是 A 中的自由变元，则 $\forall xA$ 和 $\exists xA$ 也是谓词公式．

5．只有由使用上述四条规则有限次而得到的才是谓词公式．

由定义可知，谓词公式是由原子谓词公式、命题联结词、量词以及圆括号按照上述规则组成的一个符号串．因此命题演算中的命题公式是谓词公式的一个特例．

个体变元有自由变元和约束变元之分．

例 1 "x 是整数"是一命题函数，其中有个体变元 x．由于 x 的值未定，所以对它不能判断其真假．如果 x 取值 $\sqrt{2}$，我们就得到"$\sqrt{2}$ 是整数"，这是一个假命题；如果 x 取值 5，其结果是"5 是整数"，这是一个真命题．

例 2 "$x>y$"也不是一个命题，而是一个命题函数．其中有个体变元 x，y，由于 x 和 y 的值未定，对它也不能判断其真假．

在例 1 和例 2 中，x 和 y 的值都没有确定，当我们以确定的值去作代入后，就可得到一个命题．这样的个体变元称为是**自由变元**．

约束变元是被量词所约束了的个体变元．

例 3　$\forall x$(如果 x 是苹果，则 x 是红的)。

这已经不是一个命题函数，而是一个命题。对于其中的个体变元不需要再作代人，它的含义是确定的，它断定"一切苹果都是红的"。这当然是一个假命题。

例 4　$\exists x$(x 是偶数 $\wedge x>101$)。

这也不是一个命题函数，而是一个命题。它相当于说"存在有大于101的偶数"。这是一个真命题。

例 3 和例 4 里的个体变元都是约束变元。约束变元之所以不需要作代人，是因为当变元的个体域确定以后，它的含义是确定的。

在一个谓词公式中，形如 $\forall xA(x)$ 或 $\exists xA(x)$ 的那一部分称为是公式的 **x 约束部分**。而 $A(x)$ 称为是量词 $\forall x$ 或 $\exists x$ 的**辖域**。x 在公式的 x 约束部分的任一出现都称为 x 的**约束出现**。若量词后有括号，则括号内的公式即为此量词的辖域。若量词后无括号，则量词后最短的公式为此量词的辖域。当 x 的出现不是约束出现时，称 x 的出现是**自由出现**。因此，公式中约束出现的变元是约束变元，自由出现的变元是自由变元。

例如，对于下面的谓词公式：

(1)　$\forall xP(x,y)$，

(2)　$\forall x(P(x)\rightarrow\exists yR(x,y))$，

(3)　$\exists x(P(x)\wedge Q(x))$，

(4)　$\exists xP(x)\wedge Q(x)$，

(5)　$\forall x(P(x)\rightarrow R(x))\vee\forall x(P(x)\rightarrow Q(x))$。

$\forall xP(x,y)$ 是公式 (1) 的 x 约束部分，量词 $\forall x$ 的辖域是 $P(x,y)$。变元 x 是约束变元，变元 y 是自由变元。在公式(2)中，$\forall x$ 的辖域是 $P(x)\rightarrow\exists yR(x,y)$。$\exists y$ 的辖域是 $R(x,y)$。x 和 y 两者的所有出现都是约束出现。注意区别公式(3)和公式(4)，在(3)中 $\exists x$ 的辖域是 $P(x)\wedge Q(x)$。而在 (4) 中 $\exists x$ 的辖域是 $P(x)$，x

在 $Q(x)$ 中的出现是自由出现。为避免混乱，可将公式(4)改写成 $\exists yP(y)\wedge Q(x)$。公式(5)中第一个 $\forall x$ 的辖域是 $P(x)\to R(x)$，第二个 $\forall x$ 的辖域是 $P(x)\to Q(x)$。这个公式也最好改写成

$$\forall x(P(x)\to R(x))\vee\forall y(P(y)\to Q(y)).$$

一个命题表示成谓词公式的时候与个体变元的个体域有关。例如，若要把命题"对于任一正整数，总存在一个更大的正整数"用符号来表示，如果我们考虑的是所有正整数的集合，则命题相当于"对于所有的 x，必存在一个 y，使得 y 比 x 大"。若用 $G(x,y)$ 表示 x 比 y 大，那么所给的命题可表示成 $\forall x\exists yG(y,x)$。但如果我们对 x，y 的取值范围不加限制，或者说 x，y 可以是任何个体，那么上一命题就要表示为

$$\forall x(P(x)\to\exists y(P(y)\wedge G(y,x))).$$

其中 $P(x)$ 表示"x 是正整数"。

此外，一个命题的真值也和个体域有关。例如，若用 $Q(x)$ 表示"x 是素数"，那么命题 $\forall xQ(x)$ 对于下面给出的个体域(1)取值为真，而对于(2)取值为假。

(1) $\{2,\ 5,\ 7,\ 11\}$.

(2) $\{2,\ 5,\ 7,\ 9\}$.

§9.7 谓词演算的永真公式和公式的等值

在谓词演算的公式中包含有个体变元、命题变元和谓词。当公式中的自由个体变元用其个体域中的确定的个体代入，命题变元用确定的命题代入后，原公式就变成了一个命题。这个命题有确定的真值。而这样一组代入到谓词公式中去的确定的个体和命题称为公式的一组指派。这里所给出的谓词公式包含谓词，但不包含谓词变元。即每一个谓词符号都看作是一个确定的谓词，不能随意地进行代入。

如果对于命题变元和个体变元的任意一组指派，谓词公式A的值总是为真，则我们称公式A是**永真公式**。如果对命题变元和个体变元的任意一组指派，公式A的值总是为假，则称公式A为**永假公式**或**不可满足的公式**。如果至少存在着一组指派，使公式A的值为真，则称公式A是**可满足的公式**。

如果对于它们所包含的各个命题变元和个体变元的任意一组指派，谓词公式A和B都具有相同的值，则称A和B**等值**。并记作$A \Leftrightarrow B$。因此一个公式A是永真公式相当于$A \Leftrightarrow 1$。类似地，我们也可以定义谓词公式之间的蕴含关系。即若$A \to B \Leftrightarrow 1$，则称**公式 A 蕴含公式 B**。并记作$A \Rightarrow B$。

当个体域是有限集合的时候，原则上来说，可以用真值表的方法来验证一个公式是否为永真公式，或者验证两个公式是否等值。

例如，设个体域$E=\{a_1, a_2, \cdots, a_n\}$，则包含有全称量词的谓词公式$\forall x A(x)$表示$a_1$有性质$A$，$a_2$有性质$A$，$\cdots$，$a_n$有性质$A$。因此

$$\forall x A(x) \Leftrightarrow A(a_1) \wedge A(a_2) \wedge \cdots \wedge A(a_n).$$

因为$A(a_i)$（$i=1,2,\cdots,n$）中都没有个体变元，也没有量词，所以上一合取式实际上是命题演算中的命题公式。

包含有存在量词的谓词公式$\exists x A(x)$表示a_1有性质A，或者a_2有性质A，$\cdots$，或者a_n有性质A。因此

$$\exists x A(x) \Leftrightarrow A(a_1) \vee A(a_2) \vee \cdots \vee A(a_n).$$

同样地，这一析取式也是命题演算中的命题公式。

如果一个谓词公式中包含有多个量词，则可以从里到外地用上述方法将量词逐个消去，因而使公式转换成命题演算中的命题公式。但是，当个体域中元素很多，甚至为无限集时，这个方法就变得不实际甚至不可能了。

包含有量词而不包含自由变元的谓词公式，实际上也是命题演算的公式。因此对命题演算中的所有重言式，若将其中每一个命题

变元分别用这些公式去作代入，便可得到谓词演算中的永真公式。

例如，在 $P \vee \neg P$ 和 $(P \to Q) \leftrightarrow (\neg P \vee Q)$ 中，若用 $\forall x P(x)$ 代替 P，用 $\exists x Q(x)$ 代替 Q，就得到永真公式

$$\forall x P(x) \vee \neg \forall x P(x),$$

$$(\forall x P(x) \to \exists x Q(x)) \leftrightarrow (\neg \forall x P(x) \vee \exists x Q(x)).$$

若将每一命题变元分别代换为不包含联结词的原子谓词公式，则又可得到谓词演算中的一类永真公式。例如

$$(A(x) \to B(x,y)) \leftrightarrow (\neg A(x) \vee B(x,y)),$$

$$(A(x) \vee B(x,y)) \leftrightarrow (B(x,y) \vee A(x)),$$

$$\neg(\neg C(x,y)) \leftrightarrow C(x,y).$$

在这种意义下，命题演算中所列出的一些命题公式的等值关系及蕴含关系也可以看成是谓词演算中的等值关系和蕴含关系。

此外，由于谓词演算的公式中出现了全称量词 $\forall x$ 和存在量词 $\exists x$，因此，相应地它还有一些等值关系式和蕴含关系式。其中最常见的列于表 9-3 中。

表 9-3

$\exists x(A(x) \vee B(x)) \Leftrightarrow \exists x A(x) \vee \exists x B(x)$	E_{18}
$\forall x(A(x) \wedge B(x)) \Leftrightarrow \forall x A(x) \wedge \forall x B(x)$	E_{19}
$\neg \exists x A(x) \Leftrightarrow \forall x \neg A(x)$	E_{20}
$\neg \forall x A(x) \Leftrightarrow \exists x \neg A(x)$	E_{21}
$\forall x A(x) \vee \forall x B(x) \Rightarrow \forall x(A(x) \vee B(x))$	I_{15}
$\exists x(A(x) \wedge B(x)) \Rightarrow \exists x A(x) \wedge \exists x B(x)$	I_{16}

表 9-3 中各式均可以用定义直接证明。其中 E_{20} 和 E_{21} 说明全称量词和存在量词可以相互转化，而且量词前面的否定号可以深入到辖域内。

在谓词公式中，往往有这样的情形，它的某个量词的辖域中存在着不含有被此量词所约束的个体变元的子公式。此时，可以

将这个子公式从量词的辖域中提出来。但有时量词要作适当的改变。表 9-4 列出了这一类的等值关系式。

表 9-4

$$\forall x(A \lor B(x)) \Leftrightarrow A \lor \forall xB(x)$$

$$\exists x(A \land B(x)) \Leftrightarrow A \land \exists xB(x)$$

$$\forall xA(x) \rightarrow B \Leftrightarrow \exists x(A(x) \rightarrow B)$$

$$\exists xA(x) \rightarrow B \Leftrightarrow \forall x(A(x) \rightarrow B)$$

$$A \rightarrow \forall xB(x) \Leftrightarrow \forall x(A \rightarrow B(x))$$

$$A \rightarrow \exists xB(x) \Leftrightarrow \exists x(A \rightarrow B(x))$$

表 9-4 中各等值式的证明也很容易。只要注意到，若公式 A 不含有个体变元 x，则

$$\forall xA \Leftrightarrow A, \qquad \exists xA \Leftrightarrow A.$$

§9.8 谓词演算的推理理论

利用命题公式间的各种等值关系和蕴含关系，通过一些推理规则，从已知的命题公式推出另一些新的命题公式。这是命题演算中的推理。类似地，利用谓词公式间的各种等值关系和蕴含关系，通过一些推理规则，从一些谓词公式推出另一些谓词公式，这就是谓词演算中的推理。在谓词演算中，要进行正确的推理，也必须构造一个结构严谨的形式证明，因此也要求给出一些相应的推理规则。命题演算中所使用的推理规则，都可以应用于谓词演算的推理中。除此以外，由于谓词逻辑中引进了个体词、谓词和量词等，因此又增加了一些推理规则，下面介绍几个与量词有关的推理规则：

1. US（全称特定化规则）

$$\forall xA(x) \Rightarrow A(y)$$

$A(y)$ 是将 $A(x)$ 中的 x 处处代之以 y。要求 y 在 $A(x)$ 中不约束出现。这里自由变元 y 也可以写成个体常元 c，这时 c 为个体域中任意一个确定的个体。

这个规则的意思是说，如果个体域的所有元素都具有性质 A。则个体域中的任一个元素具有性质 A。

2. **ES**（存在特定化规则）

$$\exists xA(x) \Rightarrow A(c)$$

这里 c 是个体域中的某个确定的个体。这个规则是说，如果个体域中存在有性质 A 的元素，则个体域中必有某一元素 c 具有性质 A。但是，如果 $\exists xA(x)$ 中有其它自由个体变元出现，且 x 是随其它自由个体变元的值而变，那么就不存在唯一的 c 使得 $A(c)$ 对自由个体变元的任意值都是成立的。这时，就不能应用存在特定化规则。

3. **UG**（全称一般化规则）

$$A(x) \Rightarrow \forall yA(y)$$

这个规则是说，如果个体域中任意一个个体都具有性质 A，则个体域中的全体个体都具有性质 A。这里要求 x 必须为自由变元，并且 y 不出现在 $A(x)$ 中。

4. **EG**（存在一般化规则）

$$A(c) \Rightarrow \exists yA(y)$$

这个规则是说，如果个体域中有某一元素 c 具有性质 A，则个体域中存在着具有性质 A 的元素。这里要求 y 不在 $A(c)$ 中出现。

有了上述这些规则，再加上命题演算中所给出的推理规则，我们就可以进行谓词演算中一些较为简单的推理。

下面举例说明谓词演算的推理过程。

例 1　证明 $\forall x(P(x) \to Q(x)) \wedge P(c) \Rightarrow Q(c)$

证明

(1) $\forall x(P(x)\rightarrow Q(x))$　　前提

(2) $P(c)\rightarrow Q(c)$　　(1)；US

(3) $P(c)$　　前提

(4) $Q(c)$　　(2)，(3)；I_{11}

这就是逻辑中的“三段论方法”。例如，“所有的人都是要死的，张三是人，所以张三是要死的”。

例 2　证明 $\exists x(P(x)\wedge Q(x))\Rightarrow\exists xP(x)\wedge\exists xQ(x)$

证明

(1) $\exists x(P(x)\wedge Q(x))$　　前提

(2) $P(c)\wedge Q(c)$　　(1)，*ES*

(3) $P(c)$　　(2)；I_1

(4) $Q(c)$　　(2)；I_2

(5) $\exists xP(x)$　　(3)；*EG*

(6) $\exists xQ(x)$　　(4)；*EG*

(7) $\exists xP(x)\wedge\exists xQ(x)$　　(5)，(6)，I_9

在使用*US*，*ES*，*UG*，*EG*这四条规则时，要注意严格按照它们的规定去使用，否则会推出错误的结论。我们举例来说明这一点。

例如　要求证明 $\exists xP(x)\wedge\exists xQ(x)\Rightarrow\exists x(P(x)\wedge Q(x))$

我们作如下推导：

(1) $\exists xP(x)\wedge\exists xQ(x)$　　前提

(2) $\exists xP(x)$　　(1)；I_1

(3) $\exists xQ(x)$　　(1)，I_2

(4) $P(c)$　　(2)，*ES*

(5) $Q(c)$　　(3)；*ES*

(6) $P(c)\wedge Q(c)$　　(4)，(5)；I_9

(7) $\exists x(P(x)\wedge Q(x))$　　(6)；*EG*

我们知道$(\exists xP(x)\wedge\exists xQ(x))\rightarrow\exists x(P(x)\wedge Q(x))$并不是永真公式，因此上述推导是错误的。错误在于（4）、（5）两步使用*ES*时得到的$P(c)$和$Q(c)$中的个体元素c不应该是相同的。

例 3 证明$\forall x(P(x)\vee Q(x))$、$\forall x\neg P(x)\Rightarrow\exists xQ(x)$

证明 用反证法，假设$\neg\exists xQ(x)$成立。

(1)	$\forall x\neg P(x)$	前提
(2)	$\neg P(y)$	(1)；*US*
(3)	$\neg\exists xQ(x)$	假设
(4)	$\forall x\neg Q(x)$	(3)；E_{26}
(5)	$\neg Q(y)$	(4)；*US*
(6)	$\neg P(y)\wedge\neg Q(y)$	(2)，(5)；I_9
(7)	$\neg(P(y)\vee Q(y))$	(6)；E_{10}
(8)	$\forall x(P(x)\vee Q(x))$	前提
(9)	$P(y)\vee Q(y)$	(8)；*US*
(10)	$(P(y)\vee Q(y))\wedge\neg(P(y)\vee Q(y))$	(7)，(9)；I_9

因为$(P(y)\vee Q(y))\wedge\neg(P(y)\vee Q(y))$是永假公式，所以

$$\forall x(P(x)\vee Q(x))、\forall x\neg P(x)\Rightarrow\exists xQ(x)。$$

习　　题

1. 构造下列命题公式的真值表：

(1) $\neg P\vee(Q\wedge\neg R)$；

(2) $(P\wedge\neg Q)\vee(R\wedge Q)$；

(3) $(P\rightarrow Q)\leftrightarrow(\neg P\vee Q)$；

(4) $(Q\wedge(P\rightarrow Q))\rightarrow P$；

(5) $((P\vee Q)\rightarrow(Q\wedge R))\rightarrow(P\wedge\neg R)$。

2. 下列命题公式中哪些是重言式？哪些是矛盾式？

(1) $(P\to Q)\leftrightarrow(\neg Q\to\neg P)$;

(2) $(Q\wedge(P\to Q))\to(P\to Q)$;

(3) $(\neg Q\to P)\to(P\to Q)$;

(4) $((P\vee Q)\to R)\leftrightarrow S$;

(5) $(P\wedge Q)\leftrightarrow P$;

(6) $(P\to\neg P)\to\neg P$.

3. 证明下列命题公式的等值关系：

(1) $(P\to Q)\wedge(R\to Q)\Leftrightarrow(P\vee R)\to Q$;

(2) $\neg(P\leftrightarrow Q)\Leftrightarrow(P\vee Q)\wedge\neg(P\wedge Q)$;

(3) $\neg(P\leftrightarrow Q)\Leftrightarrow(P\wedge\neg Q)\vee(\neg P\wedge Q)$;

(4) $((Q\wedge R)\to S)\wedge(R\to(P\vee S))\Leftrightarrow(R\wedge(P\to Q))\to S$;

(5) $(P\to(Q\to R))\Leftrightarrow(P\to\neg Q)\vee(P\to R)$.

4. 证明下列命题公式的蕴含关系：

(1) $P\to(Q\to R)\Rightarrow(P\to Q)\to(P\to R)$,

(2) $((P\vee\neg P)\to Q)\to((P\vee\neg P)\to R)\Rightarrow(Q\to R)$,

(3) $(Q\to(P\wedge\neg P))\to(R\to(P\wedge\neg P))\Rightarrow(R\to Q)$.

5. 求下列命题公式的主合取范式和主析取范式并判断公式是否为重言式或矛盾式：

(1) $(\neg P\vee\neg Q)\to(P\leftrightarrow\neg Q)$.

(2) $\neg(P\to Q)\leftrightarrow(P\to\neg Q)$.

(3) $(\neg R\wedge(Q\to P))\to(P\to(Q\vee R))$.

(4) $(P\to(Q\wedge R))\wedge(\neg P\to(\neg Q\wedge\neg R))$.

6. 证明：

(1) 证明 $\neg S$ 是前提 $P\to Q$、$(\neg Q\vee R)\wedge\neg R$、$\neg(\neg P\wedge S)$ 的结论。

(2) 证明 $\neg P\vee\neg Q$ 是前提 $(P\wedge Q)\to R$、$\neg R\vee S$、$\neg S$ 的结论。

(3) 证明 $R\vee S$ 是前提 $P\wedge Q$、$(P\leftrightarrow Q)\to(R\vee S)$ 的结论。

7. 证明：

(1) $\neg\exists x(P(x)\wedge Q(a))\Rightarrow\exists xP(x)\rightarrow\neg Q(a)$

(2) $\forall x(\neg P(x)\rightarrow Q(x))$、$\forall x\neg Q(x)\Rightarrow P(a)$。

(3) $\forall x(P(x)\rightarrow(Q(y)\wedge R(x)))$，$\exists xP(x)\Rightarrow Q(y)\wedge\exists x(P(x)\wedge R(x))$。

参 考 书

[1] Arthur Gill *Applied Algebra for The Computer Sciences*. Prentice-Hall Inc., 1976.

[2] J. P. Tremblay and R. Manohar, *Discrete Mathematical Structures with Applications to Computer Science*, McGraw-Hill, 1975.

[3] C. L. Liu. *Elements of Discrete Mathematics*, McGraw-Hill, 1977.

[4] D. F. Stanat and D. F. McAllister, *Discrete Mathematics in Computer Science*, Prentice-Hall Inc., 1977.

HUAZHONG NIVERSITY OF SCIENCE AND TECHNOLOGY PRESS

离散数学习题题解

LISAN SHUXUE XITI TIJIE

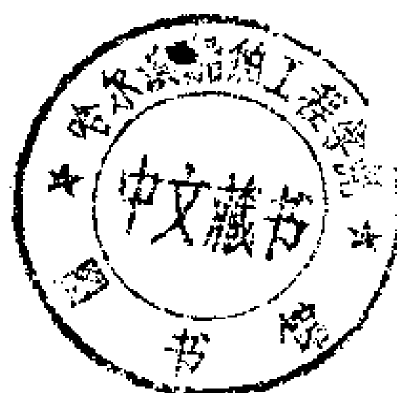
洪帆 傅小青 编

华中理工大学出版社

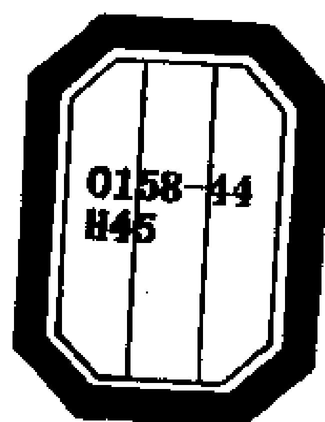


离散数学习题题解

洪 帆 傅小青 编







华中理工大学出版社

图书在版编目(CIP)数据

离散数学习题题解/洪帆　傅小青　编
武汉:华中理工大学出版社, 1999年3月
ISBN 7-5609-1904-9

Ⅰ. 离…
Ⅱ. ①洪… ②傅…
Ⅲ. 离散数学-解题
Ⅳ. O158-44

离散数学习题题解

洪帆　傅小青　编

责任编辑　李立鹏

*

华中理工大学出版社出版发行
(武昌喻家山　邮编:430074)
华中理工大学出版社照排室排版
新华书店湖北发行所经销
武汉市科普教育印刷厂印制

开本:850×1168　1/32　印张:10.125　字数:254 000
1999年3月第1版　1999年5月第2次印刷
印数:3 501-7 500
ISBN 7-5609-1904-9/O・185
定价:11.80元

前　言

本书是为配合高等院校本、专科“离散数学”课程有关教材的学习而编写的一本教学参考书。编者根据多年来在离散数学教学中所积累的经验和对学生学习中感到困难的问题，将其内容由浅入深地分为三个层次。对各章，在简短扼要地归纳其主要内容之后，首先逐一列出该章的基本知识点，对每一知识点均配有相应的实例来加以说明，以使读者正确地理解教材中的基本内容。在此基础上，针对学生对推理论证感到较为困难这一薄弱点，列举了大量的例题对读者进行逻辑推理的训练，与此同时，也使读者熟练地掌握该课程中的基本概念、基本定理、基本运算和方法。在每一部分之后，安排了一些较为复杂或有多种解题方法的题目，以帮助读者开拓思维、加深理解并学会运用所学的知识去解决各种问题。

全书共分十章，编入了359个例题，其内容侧重于课程的重点和难点。例题的解答比较详尽，编者希望它能对读者在掌握、熟悉基本概念、分析和解决问题的能力等方面有所帮助。希望读者对这些例题最好先自己进行思考，作出解答后再阅读书上的解答，这样体会深刻，收获更大。另外，读者可根据自己对离散数学课程学习掌握的情况，或采用由浅入深，循序渐进的学习方式，或直接进入第二个层次或第三个层次的学习。

本书第一章至第六章由洪帆编写，第七章至第十章由傅小青编写。对华中理工大学出版社的同志为本书的编辑出版所作的工作，在此表示衷心的感谢。

由于时间仓促，水平有限，书中错误与疏漏之处恳请读者不吝指正。

编　者

1998年10月于武汉

内容简介

本书针对“离散数学”有关教材中集合论、代数系统、图论和数理逻辑四大部分的内容，分为十章进行编排。按照基本知识点、问答与论证、解题思路与方法三个层次，由浅入深地编入了359多个具有代表性的例题。解答详实，注重基本概念的理解，分析能力的培养和逻辑思维的训练。

本书可供高等院校计算机及有关专业本、专科师生作为离散数学课程的教学和学习参考书，也是离散数学自学者的良好辅导教材。



目　　录

第一部分　集合论

第二部分　代数系统

第三部分 图论

第四部分 数理逻辑

第一部分　集合论

第一章　集　合

1.1　内容提要

1. 集合及有关概念、集合的表示法

- 集合、元素、集合的基数；
- 集合的两种表示方法：列举法和描述法；
- 两个特殊的集合：全集合和空集；
- 子集、包含集和幂集；
- 分划和细分；
- 集合的最小集标准形式和最大集标准形式.

2. 集合间的关系

- 集合间的包含关系 $B\subseteq A$；
- 集合间的真包含关系 $B\subset A$；
- 集合间的相等关系 $A=B$；
- 集合间的互补关系 $B'=A$.

3. 集合的运算

- 集合的并运算 $A\cup B$；
- 集合的交运算 $A\cap B$；

· 集合的补运算：相对补运算($B-A$)、绝对补运算($A'=U-A$)，A' 简称为 A 的补集；

· 集合运算的定律.

4. 对集合间的关系和运算进行分析和论证的工具

· 文氏图　直观、形象，可作为描述和分析的工具；

· 成员表　是根据运算的定义严格构造出来的，可作为证明的工具.

1.2 基本知识点

1. 集合的列举法和描述法

列举法是用列出集合中所有元素的方法来表示集合，描述法则是通过条件 P 来定义集合中元素的属性.

例 1-1　设全集合是整数集 I，试用列举法表示下列集合

(1) $A=\{x \mid x^2-16=0 \text{ 或 } x^4=1\}$；

(2) $B=\{x \mid x^2-10x-24<0 \text{ 且 } -5\leqslant x\leqslant 6\}$.

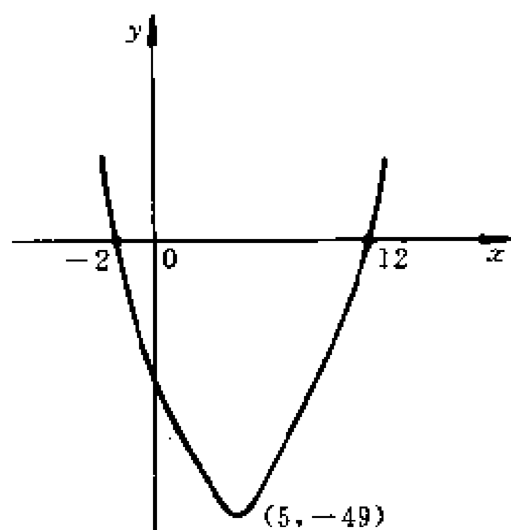


图 1-1

解　(1) 满足 $x^2-16=0$ 即 $x^2=16$ 的 x 有两个整数 $x_1=4$ 和 $x_2=-4$. 满足 $x^4=1$ 的 x 也有两个整数 $x_3=1$ 和 $x_4=-1$. 因此

$$A=\{4,-4,1,-1\}.$$

(2) 令 $y=x^2-10x-24=(x-5)^2-49$，

显然，当 $x=-2$ 和 $x=12$ 时，$y=0$，当 $x=5$ 时，y 有极小值 -49. 函数图象如图 1-1 所示. 因为 B 是全

集合 I 的子集，所以当

$$x=-1,0,1,2,\cdots,11 \text{ 时}, y<0.$$

但 x 的这些取值中，只有 8 个数满足不等式 $-5\leqslant x\leqslant 6$，因此

$$B=\{-1,0,1,2,3,4,5,6\}.$$

2. 属于关系和包含关系

"$a\in A$"表示 a 是集合 A 的一个元素. "$B\subseteq A$"表示 B 是 A 的一个子集，它意味着集合 B 中的每一个元素也是集合 A 中的元素.

在"$a\in A$"的关系中，允许 a 是一个集合，因此也可能有"$B\in A$"的关系成立，这表示集合 B 是集合 A 的元素.

例 1-2 设 $A=\{a,b,\{c\},\{a\},\{a,b\}\}$，试指出下列论断是否正确.

(1) $a\in A$；

(2) $\{a\}\in A$；

(3) $\{a\}\subseteq A$；

(4) $\varnothing\in A$；

(5) $\varnothing\subseteq A$；

(6) $b\in A$；

(7) $\{b\}\in A$；

(8) $\{b\}\subseteq A$；

(9) $\{a,b\}\in A$；

(10) $\{a,b\}\subseteq A$；

(11) $c\in A$；

(12) $\{c\}\in A$；

(13) $\{c\}\subseteq A$；

(14) $\{a,b,c\}\subseteq A$.

解 (1)、(2)、(3)、(5)、(6)、(8)、(9)、(10)、(12)正确；

(4)、(7)、(11)、(13)、(14)错误.

例 1-3 对于任意集合 A、B 和 C，下述论断是否正确？请说明理由.

(1) 若 $A\in B$，$B\subseteq C$，则 $A\in C$；

(2) 若 $A\in B$，$B\subseteq C$，则 $A\subseteq C$；

(3) 若 $A\subseteq B$，$B\in C$，则 $A\in C$；

(4) 若 $A\subseteq B$，$B\in C$，则 $A\subseteq C$.

解 (1) 正确.

因为 $B\subseteq C$，所以集合 B 的每一个元素也是集合 C 的元素，由 $A\in B$ 知 A 是 B 的一个元素，因此 A 也是 C 的一个元素，故 $A\in C$.

（2）错误.

举反例如下：设 $A=\{a\}$，$B=\{\{a\},b\}$，$C=\{\{a\},b,\{d\}\}$. 显然 $A\in B$，$B\subseteq C$，但 $A\not\subseteq C$. 因为 $a\in A$，但 $a\notin C$.

（3）和（4）都是错误的.

举反例如下：设 $A=\{a\}$，$B=\{a,b\}$，$C=\{\{a,b\},d\}$. 显然 $A\subseteq B$，$B\in C$，但 $A\notin C$. 因为集合 C 中没有元素 $\{a\}$. 又 $A\not\subseteq C$，因为集合 A 中的元素 a 不是集合 C 的元素.

3. 子集和幂集

如果集合 A 的每一个元素都是集合 B 的元素，则称 A 是 B 的子集. 记作 $A\subseteq B$. 按照这一定义，每一集合 A 是 A 自己的子集，有 $A\subseteq A$. 如果 A 是 B 的子集，而 B 中至少有一个元素不属于 A，则称 A 是 B 的真子集. 记作 $A\subset B$.

例 1-4 列出下列集合的全部子集

（1）$A=\{a,\{b\}\}$；

（2）$B=\{\varnothing\}$；

（3）$C=\varnothing$.

解 （1）因为 $\varnothing$ 是任何集合的子集，所以 $\varnothing$ 是 A 的子集. 由 A 中任意一个元素所组成的集合是 A 的子集，所以 $\{a\}$ 和 $\{\{b\}\}$ 是 A 的子集. 由 A 中任意两个元素组成的集合是 A 的子集，所以 $\{a,\{b\}\}$ 是 A 的子集，即 A 自己是 A 的子集. 因为 A 中只有两个元素，故 A 再没有其他的子集.

由上可知，A 有四个子集：$\varnothing$、$\{a\}$、$\{\{b\}\}$ 和 $\{a,\{b\}\}$.

（2）与上同样的道理，$\varnothing$ 是 B 的子集. 此外由于 B 中仅有一个元素 $\varnothing$，因此 B 仅有的另一个子集是 $\{\varnothing\}$，即 B 自己.

由上可知，B 有两个子集：$\varnothing$ 和 $\{\varnothing\}$.

(3) $\varnothing$是任何集合的子集，因此$\varnothing$也是$\varnothing$的子集，即$\varnothing$是C的子集. 因为C中没有元素，所以C不可能有其它的子集，故C只有一个子集：$\varnothing$.

由真子集的定义，对于任意集合A，除了A自身不是A的真子集外，其它子集均是A的真子集. 因此

A有三个真子集：$\varnothing$、$\{a\}$和$\{\{b\}\}$.

B有一个真子集：$\varnothing$.

C没有真子集.

集合A的幂集是以A的所有子集为元素组成的集合. 因此只要子集的概念清楚，将A的所有子集列出来，便可得到A的幂集. A的幂集记作2^A或$P(A)$.

例 1-5 求下列集合的幂集

(1) $A=\{a,\{b\},\{a,b\}\}$;

(2) $B=\{\varnothing,\{\varnothing\}\}$.

解 (1) $2^A=\{\varnothing,\{a\},\{\{b\}\},\{\{a,b\}\},\{a,\{b\}\},\{a,\{a,b\}\},\{\{b\},\{a,b\}\},\{a,\{b\},\{a,b\}\}\}$;

(2) $2^B=\{\varnothing,\{\varnothing\},\{\{\varnothing\}\},\{\varnothing,\{\varnothing\}\}\}$.

由例 1-4 和例 1-5 可以看出，当A是有限集，元素个数为n时，A的幂集也是有限集，其元素个数为2^n. 因此若用符号$\#A$表示集合A的基数，则$\#(2^A)=2^{\#A}$.

4. 集合间的包含关系和相等关系

若A是B的子集(即若$A\subseteq B$)，则称集合B包含集合A. 这时A的每一个元素也是B的元素，但B的元素不一定都是A的元素. 如果$A\subseteq B$与$B\subseteq A$同时成立，即如果A的每一个元素都是B的元素，B的每一个元素也都是A的元素，则A和B两个集合具有完全相同的元素，这时称集合A与B相等. 记作$A=B$. 因此若$A=B$，则A与B代表的是同一个集合.

例 1-6 设$A=\{i\mid i=2k,k\in N\}$;$B=\{i\mid i=2^k,k\in N\}$;$C=$

$\{2,4,6,8,\cdots\}$，试用符号“$\subseteq$”、“$\subset$”和“$=$”恰当地连结这些集合.这里 N 表示正整数集.

解 由集合 A 中元素的定义条件可知，$A=\{i \mid i$ 是正偶数$\}$，所以 $A=C$. 由集合 B 中元素的定义条件，$B=\{2,4,8,16,32,\cdots\}$ 是部分正偶数的集合，所以 $B\subseteq A$. 因为 $6\notin B$，$10\notin B$，$\cdots$，所以 B 是 A 的真子集，因此又有 $B\subset A$. 于是也有 $B\subseteq C$，$B\subset C$.

5. 集合的运算及运算定律

集合的相对补运算也称为集合的差运算. 差集 $B-A$ 是由所有属于 B 而不属于 A 的元素组成.

例 1-7 设 $A=\{2,3,\{2,3\},\varnothing\}$，求下列集合

(1) $A-\{2,3\}$；

(2) $\{\{2,3\}\}-A$；

(3) $A-\varnothing$；

(4) $A-\{\varnothing\}$.

解 (1) $A-\{2,3\}=\{\{2,3\},\varnothing\}$；

(2) $\{\{2,3\}\}-A=\varnothing$；

(3) $A-\varnothing=A$；

(4) $A-\{\varnothing\}=\{2,3,\{2,3\}\}$.

集合的差运算可转化为集合的交运算和补运算来表达.

例 1-8 设 A、B 是任意两个集合，试证明

$$A-B=A\cap B'. \tag{1-1}$$

分析 根据两集合相等的定义，若能证明 $A-B\subseteq A\cap B'$ 且 $A\cap B'\subseteq A-B$，则 $A-B=A\cap B'$ 便成立.

证 设 $u\in A-B$，则 $u\in A$ 且 $u\notin B$，即 $u\in A$ 且 $u\in B'$，因此 $u\in A\cap B'$，故 $A-B\subseteq A\cap B'$.

反之，设 $u\in A\cap B'$，则 $u\in A$ 且 $u\in B'$，即 $u\in A$ 且 $u\notin B$，由差集的定义 $u\in A-B$，因此 $A\cap B'\subseteq A-B$.

由上证得 $A-B=A\cap B'$.

运用证明两个集合互相包含的方法，一般来说可以证明任何集合恒等式的成立，但这种方法较为繁琐. 运用集合并、交、补运算的运算定律，可方便地证明集合恒等式. 若集合表达式中出现形为 $A-B$ 的差集时，可利用(1-1)式先将运算"$-$"转化为运算"$\cap$"和"$'$".

例 1-9 设 A、B、C 为任意集合，试证明

$$A\cap(B-C)=(A\cap B)-(A\cap C).$$

证 $A\cap(B-C)=A\cap(B\cap C')$ (1-1) 式

$=A\cap B\cap C'$， 结合律

又 $(A\cap B)-(A\cap C)=(A\cap B)\cap(A\cap C)'$ (1-1) 式

$=(A\cap B)\cap(A'\cup C')$ 德摩根定律

$=(A\cap B\cap A')\cup(A\cap B\cap C')$ 分配律

$=\varnothing\cup(A\cap B\cap C')$ 交换律、结合律、互补律

$=A\cap B\cap C'$， 同一律

因此 $A\cap(B-C)=(A\cap B)-(A\cap C)$.

6. 文氏图与有限集的计数

文氏图用平面上图示的方法形象地描述全集合 U 与其子集，以及全集合 U 的子集与子集之间的关系. 由于文氏图具有形象、直观的特点，因此利用文氏图可以方便地解决一些有关有限集的元素计数问题.

例 1-10 某学校举行运动会，有 100 米短跑、掷铅球和跳高三个项目. 二年级 170 人，已知有 25 人三个项目都参加了，有 62 人至少参加了两个项目. 若该年级参加比赛的总人次是 200 人次，试问有多少人没有参加任何项目？

解 (1) 用集合的概念描述上述问题.

设全集合 U 为二年级 170 人的集合，A_1 为参加 100 米短跑的

学生集合，A_2 为参加掷铅球的学生集合，A_3 为参加跳高的学生集合.

(2) 用文氏图(图 1-2)表示各个集合.

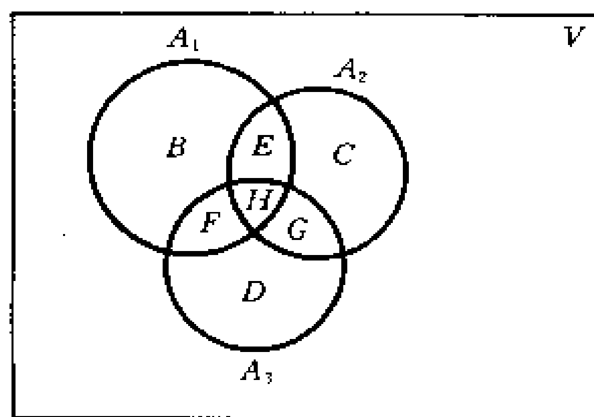


图 1-2

由题设条件和文氏图可知有关集合的基数

$$\#U = 170(\text{人})$$
$$\#H = \#(A_1 \cap A_2 \cap A_3) = 25(\text{人}),$$
$$\#(E \cup H \cup F \cup G) = 62(\text{人}).$$

(3) 计算

$$\#(E \cup F \cup G) = \#(E \cup H \cup F \cup G) - \#H$$
$$= 62 - 25 = 37(\text{人}),$$
$$25 \times 3 = 75(\text{人次}),$$
$$37 \times 2 = 74(\text{人次}),$$
$$200 - (75 + 74) = 51(\text{人次}),$$

因此 $\#B + \#C + \#D = 51(\text{人})$,

于是 $\#((A_1 \cup A_2 \cup A_3)') = \#U - \#(A_1 \cup A_2 \cup A_3)$

$$= 170 - (51 + 62)$$
$$= 57(\text{人}),$$

故该年级有 57 人没有参加任何项目.

7. 集合成员表

成员表是用表格的方式描述集合的并、交、补运算的定义，表 1-1 中任一集合 S 所标记的列中，0 表示全集合中的元素 $u\notin A$，1 表示 $u\in A$. 利用上述三个基本的成员表可以进而构造出全集合 U 的其它子集的成员表.

表 1-1

(a) A' 的成员表

A	A'
0	1
1	0

(b) $A\cup B$ 的成员表

A	B	$A\cup B$
0	0	0
0	1	1
1	0	1
1	1	1

(c) $A\cap B$ 的成员表

A	B	$A\cap B$
0	0	0
0	1	0
1	0	0
1	1	1

例 1-11 试构造集合 $(A\cup B)\cap(B\cup C)'$ 和集合 $A\cap B'$ 的成员表，通过其成员表判断这两个集合之间是否有相等关系或包含关系.

解 构造两个集合的成员表如表 1-2 所示.

表 1-2

A	B	C	$A\cup B$	$B\cup C$	$(B\cup C)'$	$(A\cup B)\cap(B\cup C)'$	B'	$A\cap B'$
0	0	0	0	0	1	0	1	0
0	0	1	0	1	0	0	1	0
0	1	0	1	1	0	0	0	0
0	1	1	1	1	0	0	0	0
1	0	0	1	0	1	1	1	1
1	0	1	1	1	0	0	1	1
1	1	0	1	1	0	0	0	0
1	1	1	1	1	0	0	0	0

集合$(A\cup B)\cap(B\cup C)'$所标记的列中，仅在第五行为1，这意味着当元素$u\in A,u\notin B$且$u\notin C$时，$u\in(A\cup B)\cap(B\cup C)'$，而在其它情形下，元素$u\notin(A\cup B)\cap(B\cup C)'$.

集合$A\cap B'$所标记的列中，第五行与第六行均为1，这意味着当元素$u\in A,u\notin B$且$u\notin C$时，$u\in A\cap B'$，当元素$u\in A,u\in C$但$u\notin B$时，也有$u\in A\cap B'$.

由上可以看出，当元素$u\in(A\cup B)\cap(B\cup C)'$时，也有$u\in A\cap B'$，但当$u\in A\cap B'$时，不一定有$u\in(A\cup B)\cap(B\cup C)'$，所以可以得出结论$(A\cup B)\cap(B\cup C)'\subseteq A\cap B'$.

8. 分划和细分

集合A的分划是由A的某些非空子集组成的集合，但这些非空子集必须满足以下两个条件：(1)任意两个子集没有公共元素；(2) 这些子集的并集恰好等于集合A.

直观地说，所谓集合A的分划就是将集合A中的元素划分成几块，使得A的每一个元素必须在某一块中，也仅在一块中.

例 1-12 设$A=\{2,3,5,8,9,16,22,25,27,35\}$，按照$A$中元素是奇数或偶数来区分，可将$A$中元素分划为两块

$$B_1=\{3,5,9,25,27,35\};$$

$$B_2=\{2,8,16,22\}.$$

因此$\Pi_1=\{B_1,B_2\}$是集合A的一个分划.

按照A中元素能被2整除，被3整除或被5整除来区分，又可将A中元素分划为三块

$$A_2=\{2,8,16,22\};$$

$$A_3=\{3,9,27\};$$

$$A_5=\{5,25,35\}.$$

因此$\Pi_2=\{A_2,A_3,A_5\}$也是集合A的一个分划.

若按照A中元素能被2整除、被3整除或被4整除来区分，

可得到 A 的如下几个非空子集

$$A_2 = \{2,8,16,22\};$$
$$A_3 = \{3,9,27\};$$
$$A_4 = \{8,16\}.$$

可令 $S=\{A_2,A_3,A_4\}$，但 S 不是 A 的分划. 原因之一是 A_2 与 A_4 有公共元素；原因之二是有些元素，如 5，25，35 不在任何子集中.

分划 Π_1 有两个分划块，分划 Π_2 有三个分划块. 我们发现 $A_2 \subseteq B_2$，$A_3 \subseteq B_1$，$A_5 \subseteq B_1$，即 Π_2 的每一个分划块都是 Π_1 的某一个分划块的子集. 因此 Π_2 是 Π_1 的细分. 如图所示，图 1-3 表示 Π_1 将 A 分划成两块，图 1-4 表示 Π_2 将 A 分划成三块. 图 1-4 可由在图 1-3 的基础上加一根分划线（图中用虚线表示）的方法，将 Π_1 中的一个分划块分成两个分划块而得到.

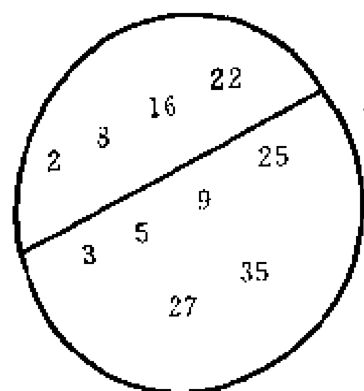


图 1-3

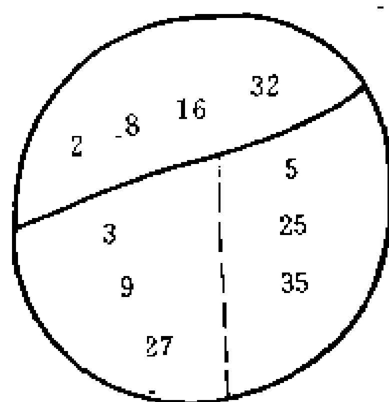


图 1-4

9. 集合的标准形式

设 A_1、A_2、…、A_r 是全集合 U 的一组子集，对 $\varnothing$、U、A_1、A_2、…、A_r 有限次地施加 $'$、$\cup$、$\cap$ 运算，所得到的集合称为是由 A_1、A_2、…、A_r 所产生的集合.

由 A_1、A_2、…、A_r 所产生的集合，可以利用集合的运算定律将其变形化为标准形式.

集合的标准形式可分为最小集标准形式和最大集标准形式.

最小集标准形式是将集合表示成 A_1、A_2、…、A_r 的不同最小集的并；最大集标准形式是将集合表示成 A_1、A_2、…、A_r 的不同最大集的交.

例 1-13 利用集合运算的定律求出集合 $(A\cap B')\cup(A'\cap(B\cup C'))$ 的最小集和最大集标准形式

解 (1) 求最小集标准形式

$$
\begin{aligned}
&(A\cap B')\cup(A'\cap(B\cup C'))\\
&\quad=(A\cap B')\cup(A'\cap B)\cup(A'\cap C')\\
&\quad=(A\cap B'\cap(C\cup C'))\cup((A'\cap B)\cap(C\cup C'))\\
&\qquad\cup((A'\cap C')\cap(B\cup B'))\\
&\quad=(A\cap B'\cap C)\cup(A\cap B'\cap C')\cup(A'\cap B\cap C)\\
&\qquad\cup(A'\cap B\cap C')\cup(A'\cap B\cap C')\\
&\qquad\cup(A'\cap B'\cap C')\\
&\quad=(A\cap B'\cap C)\cup(A\cap B'\cap C')\cup(A'\cap B\cap C)\\
&\qquad\cup(A'\cap B\cap C')\cup(A'\cap B'\cap C').
\end{aligned}
$$

(2) 求最大集标准形式

$$
\begin{aligned}
&(A\cap B')\cup(A'\cap(B\cup C'))\\
&\quad=((A\cap B')\cup A')\cap((A\cap B')\cup(B\cup C'))\\
&\quad=(A\cup A')\cap(B'\cup A')\cap(A\cup B\cup C')\\
&\qquad\cap(B'\cup B\cup C')\\
&\quad=(A'\cup B')\cap(A\cup B\cup C')\\
&\quad=(A'\cup B')\cup(C\cap C'))\cap(A\cup B\cup C')\\
&\quad=(A'\cup B'\cup C)\cap(A'\cup B'\cup C')\\
&\qquad\cap(A\cup B\cup C').
\end{aligned}
$$

利用集合的成员表也可以求集合的标准形式. 详细讨论过程请参阅参考书目[1]，下面仅通过例子给出其求标准形式的方法.

例 1-14 利用集合的成员表求出例 1-13 中集合的标准形式.

解 (1) 构造集合 $(A\cap B')\cup(A'\cap(B\cup C'))$ 的成员表

表 1-3

A	B	C	B'	$A\cap B'$	A'	C'	$B\cup C'$	$A'\cap(B\cup C')$	$(A\cap B')\cup(A'\cap(B\cup C'))$
0	0	0	1	0	1	1	1	1	1
0	0	1	1	0	1	0	0	0	0
0	1	0	0	0	1	1	1	1	1
0	1	1	0	0	1	0	1	1	1
1	0	0	1	1	0	1	1	0	1
1	0	1	1	1	0	0	0	0	1
1	1	0	0	0	0	1	1	0	0
1	1	1	0	0	0	0	1	0	0

(2) 分别找出$(A\cap B')\cup(A'\cap(B\cup C'))$所标记的列中 1 所有的行和 0 所在的行

1 所在的行是:000,010,011,100,101;

0 所在的行是:001,110,111.

(3) 根据$(A\cap B')\cup(A'\cap(B\cup C'))$所标记的列中 1 所在的行,直接写出该集合的最小集标准形式

$$\begin{aligned}&(A\cap B')\cup(A'\cap(B\cup C'))\\&=M_{000}\cup M_{010}\cup M_{011}\cup M_{100}\cup M_{101}\\&=(A'\cap B'\cap C')\cup(A'\cap B\cap C')\\&\quad\cup(A'\cap B\cap C)\cup(A\cap B'\cap C')\\&\quad\cup(A\cap B'\cap C).\end{aligned}$$

根据$(A\cap B')\cup(A'\cap(B\cup C'))$所标记的列中 0 所在的行,直接写出该集合的最大集标准形式

$$\begin{aligned}&(A\cap B')\cup(A'\cap(B\cup C'))\\&=\overline{M}_{001}\cap\overline{M}_{110}\cap\overline{M}_{111}\\&=(A\cup B\cup C')\cap(A'\cup B'\cup C)\\&\quad\cap(A'\cup B'\cup C').\end{aligned}$$

在成员表方法中,使用了二进制下标来表示最小集和最大集,这为求集合的标准形式带来了方便.而且我们可以看出,利用二进

制表示，只要求出了最小集标准形式和最大集标准形式中的任何一个，另一个亦可直接写出．即使利用集合运算的定律来求标准形式亦是如此．

1.3 问答与论证

例 1-15 给定正整数集 N 的下列子集：

$$A=\{2,5,8,9,11\};$$
$$B=\{i \mid i^3<100\};$$
$$C=\{i \mid i \text{ 可被 3 整除且 } i\leqslant 30\}.$$

求下列集合：

(1) $(A\cup B)\cap C$；　　(3) $B-(A\cup C)$；

(2) $A\cup(B\cap C)$；　　(4) $(A'\cap B)\cup C$.

解 因为
$$A=\{2,5,8,9,11\};$$
$$B=\{1,2,3,4\};$$
$$C=\{3,6,9,12,15,18,21,24,27,30\},$$

所以

(1) $(A\cup B)\cap C=\{1,2,3,4,5,8,9,11\}\cap C=\{3,9\}$；

(2) $A\cup(B\cap C)=A\cup\{3\}=\{2,3,5,8,9,11\}$；

(3) $B-(A\cup C)=B-\{2,3,5,6,8,9,11,12,15,18,21,24,27,30\}$
$=\{1,4\}$；

(4) 因为 $A'=\{1,3,4,6,7,10\}\cup\{12,13,14,\cdots\}$.

所以

$$(A'\cap B)\cup C=\{1,3,4\}\cup C$$
$$=\{1,3,4,6,9,12,15,18,21,24,27,30\}.$$

例 1-16 试定义两个集合 A、B，使得 $A\in B$ 且 $A\subseteq B$.

解 定义 $A=\{a\}$，$B=\{\{a\},a\}$，

则有　$A\in B$ 且 $A\subseteq B$.

例 1-17 设集合 A 的基数 $\#A=55$,试问

(1) A 有多少个子集?

(2) 有多少个子集的元素个数为 27?

有多少个子集的元素个数为 28?

(3) 有多少个子集的元素个数为偶数?

解 (1) 因为 $\#A=55$,所以 A 的幂集 2^A 的基数 $\#(2^A)=2^{55}$. 根据幂集的定义,A 有 2^{55}个子集.

(2) 集合是元素的组合,这些元素在集合中是无序的,因此含有 27 个元素的子集数即为从 55 个元素中取出 27 个元素的组合数,故有

$$C_{55}^{27}=\frac{55!}{27!\ 28!}\text{个子集的元素个数为 27.}$$

根据组合的基本性质 $C_n^m=C_n^{n-m}$,可知 $C_{55}^{27}=C_{55}^{28}$,所以元素个数为 28 的子集数也是$\frac{55!}{27!\ 28!}$.

(3) 由 $C_n^m=C_n^{n-m}$ 知有如下 28 个等式

$$C_{55}^0=C_{55}^{55},\quad C_{55}^1=C_{55}^{54}$$

$$C_{55}^2=C_{55}^{53}\cdots,\ C_{55}^{27}=C_{55}^{28}.$$

因为 55 是奇数,所以对任意 $m\leqslant 55$,m 和 $55-m$ 两个数中必有一个为奇数一个为偶数,因此元素个数为偶数的子集数是$\frac{2^{55}}{2}=2^{54}$.

例 1-18 设有集合 A,B,C 和 D,下述论断是否正确? 说明理由.

(1) 若 $A\subseteq B,C\subseteq D$,则$(A\cap C)\subseteq(B\cap D)$;

(2) 若 $A\subset B,C\subset D$,则$(A\cap C)\subset(B\cap D)$.

解 (1) 正确.

证 设 $u\in A\cap C$,则 $u\in A$ 且 $u\in C$,由 $A\subseteq B,C\subseteq D$,所以 $u\in B$且 $u\in D$,因此 $u\in B\cap D$,故$(A\cap C)\subseteq(B\cap D)$.

(2) 错误.

举反例如下:设

$$A = C = \{a,b,c\};$$
$$B = \{a,b,c,d\};$$
$$D = \{a,b,c,e\}.$$

显然 $$A \subset B, C \subset D,$$
$$A \cap C = \{a,b,c\} = B \cap D,$$

因此 $$A \cap C \not\subset B \cap D.$$

例 1-19 设 A、B 是任意的集合,试证明当且仅当 $A \subseteq B$ 时,$2^A \subseteq 2^B$.

证 设 $A \subseteq B$ 且 $S \in 2^A$,则 $S \subseteq A$,因为 $A \subseteq B$,所以 $S \subseteq B$,因此 $S \in 2^B$,故 $2^A \subseteq 2^B$.

反之,设 $2^A \subseteq 2^B$ 且 $u \in A$,则 $\{u\} \subseteq A$,因此 $\{u\} \in 2^A$,由 $2^A \subseteq 2^B$,所以 $\{u\} \in 2^B$,因此 $\{u\} \subseteq B$,于是 $u \in B$. 故 $A \subseteq B$.

例 1-20 设 A、B 是任意的集合

(1) 试证明 $2^A \cap 2^B = 2^{A \cap B}$;

(2) $2^A \cup 2^B = 2^{A \cup B}$ 成立吗? 为什么?

解 (1)证明 设 $S \in 2^A \cap 2^B$,则 $S \in 2^A$ 且 $S \in 2^B$,因此 $S \subseteq A$ 且 $S \subseteq B$,因而 $S \subseteq A \cap B$,即 $S \in 2^{A \cap B}$,故 $2^A \cap 2^B \subseteq 2^{A \cap B}$.

反之,设 $S \in 2^{A \cap B}$,则 $S \subseteq A \cap B$,因此 $S \subseteq A$ 且 $S \subseteq B$,因此 $S \in 2^A$ 且 $S \in 2^B$,于是 $S \in 2^A \cap 2^B$. 故 $2^{A \cap B} \subseteq 2^A \cap 2^B$.

由上知 $2^A \cap 2^B = 2^{A \cap B}$.

(2) $2^A \cup 2^B \subseteq 2^{A \cup B}$ 成立. 其证明如下:

设 $S \in 2^A \cup 2^B$,则 $S \in 2^A$ 或 $S \in 2^B$,即 $S \subseteq A$ 或 $S \subseteq B$. 因为 $A \subseteq A \cup B$,$B \subseteq A \cup B$,所以必有 $S \subseteq A \cup B$,即 $S \in 2^{A \cup B}$. 故 $2^A \cup 2^B \subseteq 2^{A \cup B}$.

$2^{A \cup B} \subseteq 2^A \cup 2^B$ 不成立.

我们可以试图来证明它成立,看会遇到什么问题.

设 $S \in 2^{A \cup B}$,则 $S \subseteq A \cup B$. 但此时我们无法推断 $S \subseteq A$,也无法推断 $S \subseteq B$,因此既不能得出 $S \in 2^A$,也不能得出 $S \in 2^B$. 例如

设 $A = \{a,c\}$,$B = \{c,b\}$.

则 $A\cup B=\{a,b,c\}$（见图 1-5）.

设 $S=\{a,b\}$，则 $S\subseteq A\cup B$，即

$S\in 2^{A\cup B}$，但 $S\nsubseteq A$，$S\nsubseteq B$，

所以 $S\notin 2^A$ 且 $S\notin 2^B$

因此 $S\notin 2^A\cup 2^B$.

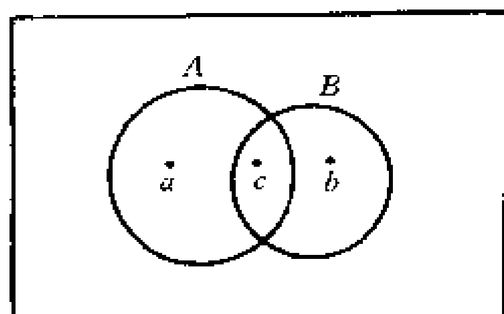


图 1-5

例 1-21 试证明对任意集合 A、B、C，等式 $(A-B)\cup(A-C)=A$ 成立的充要条件是 $A\cap B\cap C=\varnothing$.

证 必要性

设 $(A-B)\cup(A-C)=A$，因为

$$(A-B)\cup(A-C)=(A\cap B')\cup(A\cap C')$$
$$=A\cap(B'\cup C')=A\cap(B\cap C)'$$
$$=A-(B\cap C),$$

所以
$$A-(B\cap C)=A.$$

于是对任意的 $x\in A$，必有 $x\in A-(B\cap C)$，因而必有 $x\notin B\cap C$. 故 $A\cap(B\cap C)=\varnothing$.

充分性

设 $A\cap B\cap C=\varnothing$，则对任意 $x\in A$，必有 $x\notin B\cap C$，即 $x\in(B\cap C)'$，因此 $A\subseteq(B\cap C)'$. 于是

$$(A-B)\cup(A-C)=A\cap(B\cap C)'=A.$$

例 1-22 设 $\{A_1,A_2,\cdots,A_r\}$ 是集合 A 的一个分划，试证明 $A_1\cap B,A_2\cap B,\cdots,A_r\cap B$ 中所有非空集合组成 $A\cap B$ 的一个分划.

证 因为对任意的 $i(1\leqslant i\leqslant r)$，$A_i\subseteq A$，所以 $A_i\cap B\subseteq A\cap B$，即所有 $A_i\cap B$ 都是 $A\cap B$ 的子集.

又对于任意 $i\neq j(1\leqslant i,j\leqslant r)$，有

$$(A_i\cap B)\cap(A_j\cap B)=(A_i\cap A_j)\cap B=\varnothing\cap B=\varnothing;$$

$$(A_1\cap B)\cup(A_2\cap B)\cup\cdots\cup(A_r\cap B)$$

$$=(A_1 \cup A_2 \cup \cdots \cup A_r) \cap B = A \cap B.$$

由上可知,$A_1 \cap B$、$A_2 \cap B$、…、$A_r \cap B$ 中所有非空集合构成 $A \cap B$ 的一个分划.

例 1-23 设有集合 A,B,且 $A \cap B = A$,求联立方程组

$$\begin{cases} x \cup A = B; \\ x \cap A = \varnothing \end{cases}$$

的解,并证明此解是唯一的.

解 由 $A \cap B = A$ 可知 $A \cup B = B$. 令 $x = B - A$,因为

$$\begin{aligned}(B - A) \cup A &= (B \cap A') \cup A = (B \cup A) \cap (A' \cup A) \\ &= (B \cup A) \cap U = A \cup B = B,\end{aligned}$$

$$(B - A) \cap A = (B \cap A') \cap A = \varnothing,$$

所以集合 $B - A$ 是联立方程组的解.

假设 x_1 和 x_2 均是联立方程组的解,则

$$x_1 \cup A = x_2 \cup A, x_1 \cap A = x_2 \cap A.$$

于是

$$\begin{aligned}x_1 &= x_1 \cap (x_1 \cup A) = x_1 \cap (x_2 \cup A) \\ &= (x_1 \cap x_2) \cup (x_1 \cap A) = (x_1 \cap x_2) \cup (x_2 \cap A) \\ &= x_2 \cap (x_1 \cup A) = x_2 \cap (x_2 \cup A) = x_2,\end{aligned}$$

故 $B - A$ 是联立方程组唯一的解.

例 1-24 设 A、B、C 是任意集合,运用集合运算定律证明:

$$\begin{aligned}&(A \cup B) \cap (B \cup C) \cap (C \cup A) \\ &= (A \cap B) \cup (B \cap C) \cup (C \cap A).\end{aligned}$$

证 $(A \cup B) \cap (B \cup C) \cap (C \cup A)$

$$\begin{aligned}&= ((A \cup B) \cap (B \cup C)) \cap (C \cup A) \\ &= (B \cup (A \cap C)) \cap (C \cup A) \\ &= (B \cap (A \cup C)) \cup ((A \cap C) \cap (A \cup C)) \\ &= (A \cap B) \cup (B \cap C) \cup (A \cap C \cap A) \cup (A \cap C \cap C) \\ &= (A \cap B) \cup (B \cap C) \cup (A \cap C).\end{aligned}$$

例 1-25 设 A_i 为某些实数的集合,定义为:

$$A_0 = \{a \mid a < 1\};$$

$$A_i = \left\{a \mid a \leqslant 1 - \frac{1}{i}\right\} \quad (i = 1, 2, \cdots).$$

试证明
$$\bigcup_{i=1}^{\infty} A_i = A_0.$$

证 设 $a \in \bigcup_{i=1}^{\infty} A_i$，则必存在正整数 k，使得 $a \in A_k$，因此有 $a \leqslant 1 - \frac{1}{k}$，于是 $a < 1$，故 $a \in A_0$.

另一方面，设 $a \in A_0$，则有 $a < 1$，若 $a \leqslant 0$，则有 $a \in A_1$，因此 $a \in \bigcup_{i=1}^{\infty} A_i$；若 $0 < a < 1$，则令 $b = 1 - a$，$a = 1 - b = 1 - \frac{1}{\frac{1}{b}}$，令 $k = [\frac{1}{b}] + 1$(其中$[\frac{1}{b}]$表示$\frac{1}{b}$的整数部分)，则有$\frac{1}{\frac{1}{b}} > \frac{1}{k}$，因此 $a = 1 - \frac{1}{\frac{1}{b}} < 1 - \frac{1}{k}$，即 $a \in A_k$，于是 $a \in \bigcup_{i=1}^{\infty} A_i$.

由上可知$\bigcup_{i=1}^{\infty} A_i = A_0$.

例 1-26 设 $A_1, A_2, \cdots, A_r$ 为全集合 U 的子集，试问 $A_1, A_2, \cdots, A_r$ 至多能产生多少个不同的集合？

解法一 构造由 A_1、A_2、$\cdots$、A_r 所产生的集合的成员表，显然该成员表由 2^r 个行所组成. 在该成员表中不同的列可由 2^r 位的二进制数 $00\cdots0 \sim 11\cdots1$ 分别表示，而不同的列所标记的集合是不相同的，因此由 A_1、A_2、$\cdots$、A_r 至多可产生 2^{2^r} 个不同的集合.

解法二 由 A_1、A_2、$\cdots$、A_r 可产生 2^r 个最小集，而由 A_1、A_2、$\cdots$、A_r 所产生的每个非空集合都可唯一地表示为由 A_1、A_2、$\cdots$、A_r 所产生的不同最小集的并集；反之，由 A_1、A_2、$\cdots$、A_r 所产生的任意不同最小集的并集，必将表示一个由 A_1、A_2、$\cdots$、A_r 所产生的集合. 因此由 A_1、A_2、$\cdots$、A_r 所产生的集合至多为

$$C_{2^r}^0 + C_{2^r}^1 + C_{2^r}^2 + \cdots + C_{2^r}^{2^r} = 2^{2^r}$$

个.

第二章　关　系

2.1　内容提要

1. 集合的笛卡尔积

- 有序 n 元组 $(a_1,a_2,\cdots,a_n)$；
- 有序二元组(亦称为序偶) (a,b)；
- n 个集合的笛卡尔积

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1,a_2,\cdots,a_n) \mid a_i \in A_i,\ i = 1,2,\cdots,n\};$$

- 两个集合的笛卡尔积

$$A \times B = \{(a,b) \mid a \in A, b \in B\}.$$

2. 关系

- 由集合 A 到集合 B 的关系；
- 集合 A 上的关系；
- 恒等关系和普遍关系；
- 关系的逆关系；
- 复合关系；
- 集合 A 上关系 ρ 的传递闭包、对称闭包和自反闭包.

3. 关系的表示方法

- 集合表示法：列举法和描述法；
- 矩阵表示法：用矩阵表示由有限集 A 到有限集 B 的关系；
- 关系图表示法：用有向图表示有限集 A 上的关系；

· 次序图：用无向图来特定地表示有限集 A 上的偏序关系.

4. 关系的复合运算和闭包运算

· 由给定的关系 ρ_1 和 ρ_2，求复合关系 $\rho_1 \cdot \rho_2$；
· 由给定的集合 A 上的关系 ρ，求复合关系 ρ^n；
· 由给定的集合 A 上的关系 ρ，求传递闭包 ρ^+、求对称闭包 $S(\rho)$、求自反闭包 $r(\rho)$.

5. 集合 A 上关系的性质

· 集合 A 上的自反关系；
· 集合 A 上的对称关系；
· 集合 A 上的反对称关系；
· 集合 A 上的可传递的关系.
上述这些具有特殊性质的关系的定义及判别.

6. 集合 A 上两类重要的关系

· 等价关系、等价类和等价分划；
· 偏序关系、全序和良序.

2.2 基本知识点

1. 有序 n 元组与笛卡尔积

本章讨论关系，而关系的概念是通过有序 n 元组和笛卡尔积来定义的，因此读者应先将这两个概念理解清楚. 因为主要讨论二元关系，所以有序二元组和两个集合的笛卡尔积是其重点.

有序 n 元组与 n 个元素的集合是两个不同的概念，不同在于集合中这 n 个元素是无序的，而在有序 n 元组中，必须对这 n 个元素指定一个次序. 因此对任意给定的 n 个个体，他们只能组成一个

n 元素的集合，但却可以组成 $n!$ 个不同的有序 n 元组.

例 2-1 集合 $\{1,3,5,9\}=\{3,9,5,1\}=\{9,5,1,3\}$；但有序四元组 $(1,3,5,9)\neq(3,9,5,1)\neq(9,5,1,3)$.

n 个集合的笛卡尔积是一个以有序 n 元组为元素的集合，因此两个集合的笛卡尔积就是一个以序偶为元素的集合.

例 2-2 设 $A=\{1,3\}$，$B=\{1,2,4\}$，则

$A\times B=\{(1,1),(1,2),(1,4),(3,1),(3,2),(3,4)\}$；

$B\times A=\{(1,1),(2,1),(4,1),(1,3),(2,3),(4,3)\}$.

注意到 $(1,2)\neq(2,1)$，$(1,4)\neq(4,1)$，…，所以 $A\times B\neq B\times A$，即笛卡尔积不满足交换律.

2. 由集合 A 到集合 B 的关系

笛卡尔积 $A_1\times A_2\times\cdots\times A_n$ 的任意一个子集都称作是集合 A_1、A_2、…、A_n 上的一个 n 元关系. 我们特别关心的是 $n=2$ 的情形，即笛卡尔积 $A\times B$ 的任意一个子集都称作是集合 A、B 上的一个二元关系，由于 $A\times B\neq B\times A$，为区别起见，我们称它为由 A 到 B 的一个二元关系，并简称为由 A 到 B 的关系.

例 2-3 设 $A=\{1,2,4,7,8\}$，$B=\{2,3,5,7\}$，定义由 A 到 B 的关系

$$\rho=\left\{(a,b)\mid \frac{a+b}{5}\text{是整数}\right\},$$

试问 ρ 由哪些序偶组成？

解 根据 ρ 的定义，ρ 中的序偶 (a,b) 应满足如下三个条件：1) $a\in A$；2) $b\in B$；3) $a+b$ 能被 5 整除. 于是

$$\rho=\{(2,3),(7,3),(8,2),(8,7)\}.$$

集合 A、B 的基数分别是 $\#A=5$，$\#B=4$，因此笛卡尔积 $A\times B$ 的基数 $\#(A\times B)=\#A\times\#B=20$. 即集合 $A\times B$ 由所有 20 个可能的序偶组成. 而 ρ 中的四个序偶只是其中的一部分，即 $\rho\subseteq A\times B$. $A\times B$ 还有许多其它的子集，如 $\{(1,3),(2,5),(4,7),(8,$

7)}、∅、$A\times B$ 等均可看作是由 A 到 B 的关系.

例 2-4 设有集合 A、B，$\#A=n$，$\#B=m$，试问由 A 到 B 有多少个不同的关系?

解 因为笛卡尔积 $A\times B$ 的任意一个子集都称作是由 A 到 B 的一个关系，所以该问题等价于计算 $A\times B$ 有多少个子集. 由幂集的定义，该问题又等价于计算 $A\times B$ 的幂集的基数是多少.

$$\#(2^{A\times B}) = 2^{\#(A\times B)} = 2^{\#A\times\#B} = 2^{n\cdot m},$$

故由 A 到 B 有 2^{nm} 个不同的关系.

若集合 A 和 B 中至少有一个是无限集，则 $A\times B$ 是无限集. 因此 $A\times B$ 有无限多个子集，这也就意味着由 A 到 B 有无限多个不同的关系.

3. 集合 A 上的关系

如果对上述由 A 到 B 的关系的含义理解清楚了，那么集合 A 上的关系也就不难理解，因为它只不过是当 $B=A$ 时，由 A 到 B 的关系的一种特殊情形，是一个由 A 到 A 自己的关系.

例 2-5 设 $A=\{2,3,4,5,9,25\}$，定义 A 上的关系 ρ，对于任意的 $a,b\in A$，当且仅当 $(a-b)^2\in A$ 时，有 $a\rho b$，试问 ρ 由哪些序偶组成?

解 根据 ρ 的定义，ρ 中的序偶 (a,b) 应满足以下三个条件：1) $a\in A$；2) $b\in A$；3) $(a-b)^2\in A$. 因此

$$\rho = \{(2,4),(4,2),(2,5),(5,2),(3,5),(5,3),(4,9),(9,4)\}.$$

4. 关系的定义域和值域

设 ρ 是由 A 到 B 的一个关系，我们称 A 的子集

$$D_\rho = \{a \mid a\in A, \text{存在 } b\in B \text{ 使得 } (a,b)\in\rho\}$$

为关系 ρ 的定义域. 称 B 的子集

$$R_\rho = \{b \mid b\in B, \text{存在 } a\in A \text{ 使得 } (a,b)\in\rho\}$$

为关系 ρ 的值域.

例 2-6 设 $\rho_1=\{(1,2),(2,4),(3,3)\}$，$\rho_2=\{(1,3),(2,4),(4,2)\}$，试求出 D_{ρ_1}、D_{ρ_2}、$D_{\rho_1\cup\rho_2}$、R_{ρ_1}、R_{ρ_2}和 $R_{\rho_1\cap\rho_2}$.

解 题目没有告诉我们 ρ_1 和 ρ_2 是由什么集合到什么集合的关系. 这对于我们解答此题是无关紧要的. 事实上，不论 ρ_1 和 ρ_2 是定义在什么样的集合上的关系，根据 D_ρ 和 R_ρ 的定义均有

$$D_{\rho_1}=\{1,2,3\},\quad R_{\rho_1}=\{2,3,4\};$$

$$D_{\rho_2}=\{1,2,4\},\quad R_{\rho_2}=\{2,4,3\};$$

又因为 $\rho_1\cup\rho_2=\{(1,2),(2,4),(3,3),(1,3),(4,2)\}$;

$$\rho_1\cap\rho_2=\{(2,4)\},$$

所以 $D_{\rho_1\cup\rho_2}=\{1,2,3,4\}$；$R_{\rho_1\cap\rho_2}=\{4\}$.

5. 逆关系

若 ρ 是由集合 A 到集合 B 的关系，则 ρ 的逆关系 $\tilde{\rho}$（有的记作 ρ^{C}，有的记作 ρ^{-1}）是由集合 B 到集合 A 的关系. 若 ρ 是集合 A 上的关系，则 ρ 的逆关系 $\tilde{\rho}$ 也是集合 A 上的关系.

如何由关系 ρ 求逆关系 $\tilde{\rho}$ 呢? 只要将 ρ 中所有的序偶 (a,b) 改成序偶 (b,a) 便得到 $\tilde{\rho}$. 因此 $\tilde{\rho}$ 和 ρ 具有相同个数的序偶，只不过每一个序偶中，两个元素的位置要互换. 由此也可看出 ρ 与 $\tilde{\rho}$ 互为逆关系.

例 2-7 例 2-3 中由集合 A 到 B 的关系 ρ 的逆关系

$$\tilde{\rho}=\{(3,2),(3,7),(2,8),(7,8)\},$$

它是一个由集合 B 到 A 的关系.

例 2-5 中集合 A 上的关系 ρ 的逆关系 $\tilde{\rho}$ 也是 A 上的关系

$\tilde{\rho}=\{(4,2),(2,4),(5,2),(2,5),(5,3),(3,5),(9,4),(4,9)\}$,

在这里 $\tilde{\rho}=\rho$，这是巧合. 一般情形下，$\tilde{\rho}\neq\rho$.

例如，在例 2-5 的集合 A 上若定义 $\rho=\{(a,b)\mid a-b>4\}$，则

$\rho=\{(9,2),(9,3),(9,4),(25,2),(25,3),(25,4),(25,5),(25,9)\}$,

求出 $\tilde{\rho}$后，你会发现 $\tilde{\rho}\neq\rho$.

6. 复合关系

若 ρ_1 是由集合 A 到 B 的关系，ρ_2 是由集合 B 到 C 的关系，那么我们可以根据 ρ_1 和 ρ_2 定义出一个由集合 A 到 C 的新关系，记作 $\rho_1\cdot\rho_2$. 定义的方法是，对于集合 A 中任意元素 a 和集合 C 中任意元素 c，如果在集合 B 中至少存在一个元素 b，使得同时有 $(a,b)\in\rho_1$ 和 $(b,c)\in\rho_2$，则定义 $(a,c)\in\rho_1\cdot\rho_2$. 如果对于 $a\in A$ 和 $c\in C$，满足上述条件的元素 $b\in B$ 不存在，则 $(a,c)\notin\rho_1\cdot\rho_2$. 这样产生的关系 $\rho_1\cdot\rho_2$ 就称作是关系 ρ_1 和 ρ_2 的复合关系. 我们常将它简记作 $\rho_1\rho_2$.

例 2-8 设有集合 $A=\{4,5,8,15\}$，$B=\{3,4,5,9,11\}$，$C=\{1,6,8,13\}$，ρ_1 是由 A 到 B 的关系，ρ_2 是由 B 到 C 的关系，分别定义为

$$\rho_1=\{(a,b)\mid |b-a|=1\},$$

$$\rho_2=\{(b,c)\mid |b-c|=2\text{ 或 }|b-c|=4\}.$$

试求复合关系 $\rho_1\cdot\rho_2$.

解 由题意知

$$\rho_1=\{(4,3),(4,5),(5,4),(8,9)\},$$

$$\rho_2=\{(3,1),(4,6),(4,8),(5,1),(9,13),(11,13)\}.$$

根据复合关系的定义

$$\rho_1\cdot\rho_2=\{(4,1),(5,6),(5,8),(8,13)\}.$$

关系 ρ_1、ρ_2 以及复合关系 $\rho_1\cdot\rho_2$ 如图 2-1 所示.

7. 逆关系与复合关系

例 2-9 对于例 2-8 中的关系 ρ_1、ρ_2 和复合关系 $\rho_1\cdot\rho_2$，分别求出其逆关系 $\tilde{\rho}_1$、$\tilde{\rho}_2$ 和 $\widetilde{\rho_1\cdot\rho_2}$. 再求出复合关系 $\widetilde{\rho_2\cdot\rho_1}$. 试问 $\widetilde{\rho_1\cdot\rho_2}$ 与 $\tilde{\rho}_2\cdot\tilde{\rho}_1$ 有什么关系?

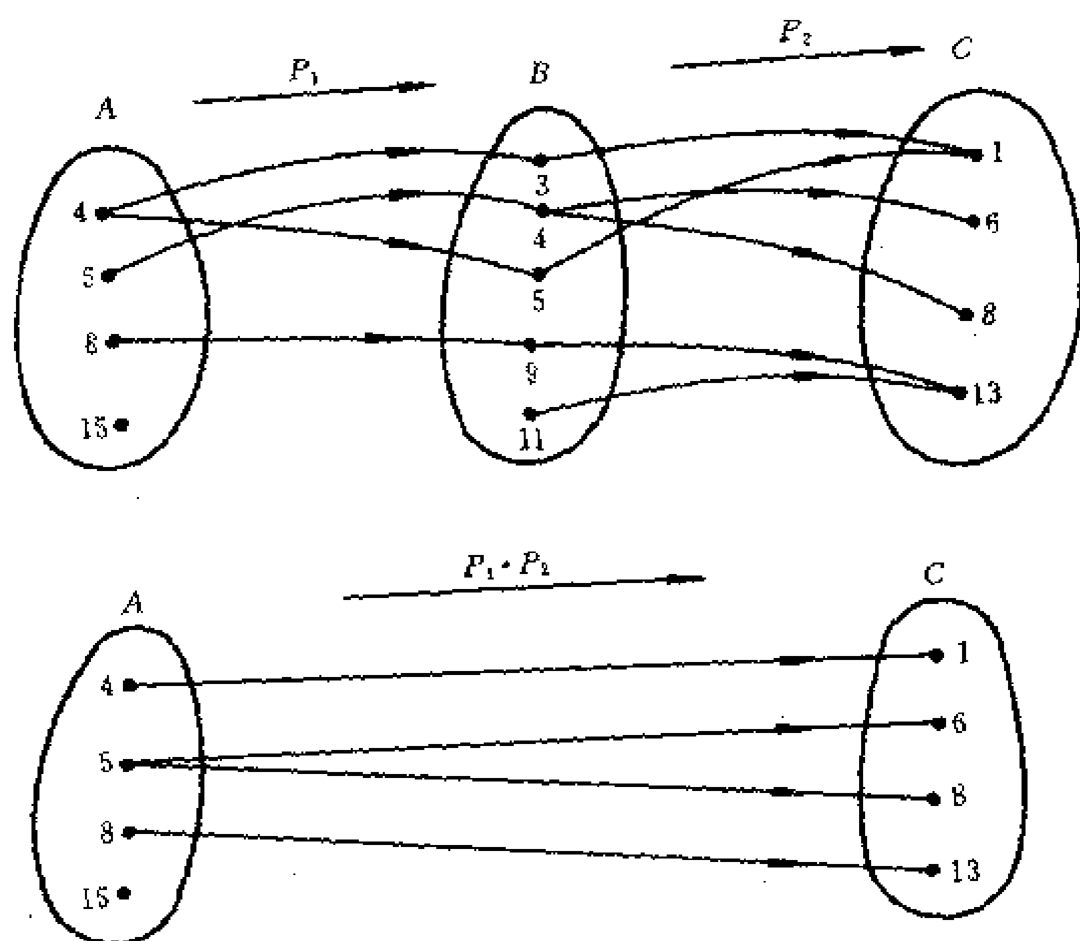


图 2-1

解 根据逆关系的定义，$\tilde{\rho}_1$ 是由 B 到 A 的关系，$\tilde{\rho}_2$ 是由 C 到 B 的关系，$\widetilde{\rho_1\cdot\rho_2}$ 是由 C 到 A 的关系. 它们分别为

$$\tilde{\rho}_1=\{(3,4),(5,4),(4,5),(9,8)\},$$

$$\tilde{\rho}_2=\{(1,3),(6,4),(8,4),(1,5),(13,9),(13,11)\},$$

$$\widetilde{\rho_1\cdot\rho_2}=\{(1,4),(6,5),(8,5),(13,8)\}.$$

根据复合关系的定义，$\tilde{\rho}_2\cdot\tilde{\rho}_1$ 是由 C 到 A 的关系且

$$\tilde{\rho}_2\cdot\tilde{\rho}_1=\{(1,4),(6,5),(8,5),(13,8)\}.$$

$\widetilde{\rho_1\cdot\rho_2}$ 与 $\tilde{\rho}_2\cdot\tilde{\rho}_1$ 都是由 C 到 A 的关系，且由完全相同的四个序偶所组成，因此 $\widetilde{\rho_1\cdot\rho_2}=\tilde{\rho}_2\cdot\tilde{\rho}_1$. 即 $\widetilde{\rho_1\cdot\rho_2}$ 与 $\tilde{\rho}_2\cdot\tilde{\rho}_1$ 表示的是由

C 到 A 的同一个关系.

在一般情形下,等式$\widetilde{\rho_1 \cdot \rho_2}=\widetilde{\rho_2} \cdot \widetilde{\rho_1}$ 也是成立的,我们将在后面给出其证明(参见本章例 2-26).

8. 集合 A 上的复合关系 ρ^n

设 ρ 是集合 A 上的关系,根据复合关系的定义,ρ 和 ρ 的复合关系 ρ^2 也是 A 上的关系.同样的道理,$\rho^3,\rho^4,\cdots$均是 A 上的关系.因此若 ρ 是集合 A 上的关系,则对于任意的正整数 n,ρ^n 是 A 上的关系.

例 2-10 设 $A=\{a,b,c,d,e\}$,A 上的关系 ρ 定义为

$$\rho=\{(a,b),(b,a),(a,c),(c,e),(d,b)\},$$

试对所有的 $n\in N$(N 表示正整数集),求出 ρ^n.

解 $\rho^2=\rho\cdot\rho=\{(a,a),(a,e),(b,b),(b,c),(d,a)\}$,

由于关系的复合运算满足结合律,因此 ρ^3 可以看作是 $\rho\cdot\rho^2$,也可看作是 $\rho^2\cdot\rho$.

$$\rho^3=\rho\cdot\rho^2=\{(a,b),(a,c),(b,a),(b,e),(d,b),(d,c)\}$$

类似地,$\rho^4=\rho\cdot\rho^3=\rho^2\cdot\rho^2=\rho^3\cdot\rho$

$$=\{(a,a),(a,e),(b,b),(b,c);(d,a),(d,e)\}$$

$$\rho^5=\rho\cdot\rho^4=\rho^2\cdot\rho^3=\rho^3\cdot\rho^2=\rho^4\cdot\rho$$

$$=\{(a,b),(a,c),(b,a),(b,e),(d,b),(d,c)\},$$

我们发现 $\rho^5=\rho^3$,根据复合关系的定义便有

$$\rho^6=\rho^5\cdot\rho=\rho^3\cdot\rho=\rho^4,$$

$$\rho^7=\rho^6\cdot\rho=\rho^4\cdot\rho=\rho^5=\rho^3,$$

$$\rho^8=\rho^7\cdot\rho=\rho^5\cdot\rho=\rho^6=\rho^4,\cdots$$

于是有

$$\rho^3=\rho^5=\rho^7=\rho^9=\cdots$$

$$\rho^4=\rho^6=\rho^8=\rho^{10}=\cdots$$

即当 $n\geqslant 3$ 时,

$$\rho^{2n-1}=\rho^3,$$

$$\rho^{2n}=\rho^4.$$

由例 2-10 我们看出,对于集合 A 上的关系 ρ,虽然经复合运

算可得到无限多个复合关系

$$\rho^2, \rho^3, \rho^4, \cdots$$

但在这些关系中,可能有许多关系是相同的.

9. 集合 A 上关系 ρ 的传递闭包 ρ^+

集合 A 上关系 ρ 的传递闭包记作 ρ^+(有的记作 $t(\rho)$),它也是集合 A 上的一个关系,由下式定义

$$\rho^+ = \bigcup_{i=1}^{\infty} \rho^i.$$

即 $\rho^+ = \rho \cup \rho^2 \cup \rho^3 \cup \cdots$ 是 A 上形为 ρ^i 的无限多个关系的并集.

如果 A 是无限集,则 $A \times A$ 也是无限集,于是 $A \times A$ 的子集也就有无限多个. 因此 A 上有无限多个不同的关系. 另外 A 上的关系有些也可能是无限集. 这样一来 ρ^+ 也就有可能是一个无限集,因此要求出 ρ^+ 中的所有序偶可能是一件困难的事情. 但是,如果 A 是有限集,则 $A \times A$ 也是有限集,于是 $A \times A$ 上就只有有限个不同的关系. 这样一来尽管形式上看 ρ^+ 是无限多个关系的并集,但实际上只可能是有限个关系的并. 因此在这种情形下,我们可以将 ρ^+ 中的全部序偶求出来.

例 2-11 试求出例 2-10 中关系 ρ 的传递闭包 ρ^+.

解 按定义 $\rho^+ = \bigcup_{i=1}^{\infty} \rho^i$,但因为在无穷序列

$$\rho, \rho^2, \rho^3, \rho^4, \rho^5, \rho^6, \rho^7, \cdots$$

中,除 ρ、ρ^2、ρ^3 和 ρ^4 这四个关系互不相同外,其它关系均与关系 ρ^3 或 ρ^4 相同,由集合并运算的等幂律

$$\begin{aligned}\rho^+ &= \rho \cup \rho^2 \cup \rho^3 \cup \rho^4 \\ &= \{(a,a),(a,b),(a,c),(a,e),(b,a),(b,b),(b,c), \\ &\quad (b,e),(c,e),(d,a),(d,b),(d,c),(d,e)\}.\end{aligned}$$

10. 关系的表示方法

(1) 集合表示法

因为关系是一个集合，因此可以用集合的列举法或描述法来表示它. 在前面的例题中，我们已多次采用了这两种方法.

例如，例 2-3 中定义的由 A 到 B 的关系

$$\rho = \left\{(a,b)\,\middle|\,\frac{a+b}{5}\text{是整数}\right\}$$

用的就是描述法，而例 2-10 中定义的关系 ρ 用的是列举法.

(2) 矩阵表示法

若 ρ 是由有限集 A 到有限集 B 的关系，则可以用一个 $\#A$ 行，$\#B$ 列的矩阵来表示 ρ. 该矩阵称为是 ρ 的关系矩阵. 记作 M_ρ. M_ρ 的第 i 行 j 列的元素 $r_{ij}=1$ 或 0，它取决于 $(a_i,b_j)\in\rho$ 或 $(a_i,b_j)\notin\rho$.

例 2-12 设 $A=\{5,4,35,49\}$，$B=\{8,15,7\}$，由 A 到 B 的关系 P 定义为

$$\rho = \{(a,b)\ a\text{ 与 }b\text{ 互素}\},$$

试写出 ρ 的关系矩阵 M_ρ.

解 由定义 $\rho=\{(5,8),(5,7),(4,15),(4,7),(35,8),(49,8),(49,15)\}$，所以关系矩阵

$$M_\rho = \begin{array}{c} \\ 5 \\ 4 \\ 35 \\ 49 \end{array}\begin{array}{c} \begin{array}{ccc} 8 & 15 & 7 \end{array} \\ \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix} \end{array}.$$

(3) 图表示法

若 ρ 是定义在有限集 A 上的一个关系，则 ρ 又可以用一个有向图来表示，此有向图称为 ρ 的关系图. 图中每一个结点与 A 的一个元素对应，图中的每一条边与 ρ 的一个序偶对应.

例 2-13 设 $A=\{5,4,35,49\}$，定义 A 上的关系

$$\rho = \{(a_i,a_j)\,|\,a_i + a_j \leqslant 53\},$$

试画出 ρ 的关系图.

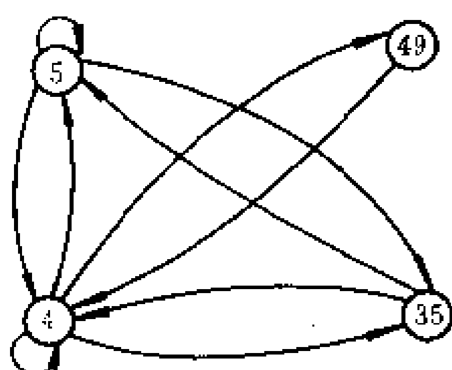


图 2-2

解　由定义 $\rho=\{(5,5),(5,4),(5,35),(4,5),(4,4),(4,35),(4,49),(35,5),(35,4),(49,4)\}$.
因此 ρ 的关系图如图 2-2。

11. 如何利用关系的各种表示方法进行关系的运算

(1) 关系的并、交、补和差运算

例 2-14　设 $A=\{4,6,9,10\}$，ρ_1 和 ρ_2 是 A 上的两个关系

$$\rho_1=\left\{(a,b)\middle|\frac{a-b}{2}\text{是正整数}\right\},$$

$$\rho_2=\left\{(a,b)\middle|\frac{a-b}{3}\text{是正整数}\right\},$$

试求 $\rho_1\cup\rho_2$、$\rho_1\cap\rho_2$、ρ'_1、$\rho_1-\rho_2$.

解　$\rho_1=\{(6,4),(10,4),(10,6)\}$;

$$\rho_2=\{(9,6),(10,4)\};$$

因此　$\rho_1\cup\rho_2=\{(6,4),(9,6),(10,4),(10,6)\}$;

$$\rho_1\cap\rho_2=\{(10,4)\};$$

$$\begin{aligned}\rho'_1&=(A\times A)-\rho_1\\&=\{(4,4),(4,6),(4,9),(4,10),(6,6),(6,9),\\&\quad(6,10),(9,4),(9,6),(9,9),(9,10),(10,9),(10,10)\};\end{aligned}$$

$$\rho_1-\rho_2=\{(6,4),(10,6)\}.$$

因为 ρ_1 和 ρ_2 都是 A 上的关系，$\rho_1\subseteq A\times A$，$\rho_2\subseteq A\times A$，所以 $\rho_1\cup\rho_2\subseteq A\times A$，$\rho_1\cap\rho_2\subseteq A\times A$，$\rho'_1\subseteq A\times A$，$\rho_1-\rho_2\subseteq A\times A$，即 $\rho_1\cup\rho_2$，$\rho_1\cap\rho_2$，ρ'_1，$\rho_1-\rho_2$ 也都是集合 A 上的关系. 对这些关系也可用描述法定义如下：

$$\rho_1\cup\rho_2=\left\{(a,b)\middle|\frac{a-b}{2}\text{是正整数或者}\frac{a-b}{3}\text{是正整数}\right\};$$

$$\rho_1\cap\rho_2=\left\{(a,b)\middle|\frac{a-b}{2}\text{和}\frac{a-b}{3}\text{均为正整数}\right\};$$

$$\rho'_1=\left\{(a,b)\middle|\frac{a-b}{2}\text{不是正整数}\right\};$$

$$\rho_1-\rho_2=\left\{(a,b)\middle|\frac{a-b}{2}\text{是正整数，但}\frac{a-b}{3}\text{不是正整数}\right\}.$$

（2）关系的复合运算

关系的各种表示方法都可以用来进行关系的复合运算.

例 2-15 设 $A=\{a,b,c,d\}$，A 上的关系

$$\rho=\{(a,a),(a,b),(b,d),(c,a),(d,c)\},$$

试求复合关系 ρ^2.

解 方法一

根据关系 ρ 中所列出的序偶，按复合关系的定义求出 ρ^2 中的序偶. 只要有 $(x,y)\in\rho$ 和 $(y,z)\in\rho$，便有 $(x,z)\in\rho^2$. 因此

$$\rho^2=\{(a,a),(a,b),(a,d),(b,c),(c,a),(c,b),(d,a)\}.$$

这里特别要注意 $(a,a)\in\rho^2$ 不要遗漏，它是由 $(a,a)\in\rho$，$(a,a)\in\rho$ 而得来的.

方法二

构造出 ρ 的关系矩阵 M_ρ，利用 ρ^2 的关系矩阵 $M_{\rho^2}=M_\rho\cdot M_\rho$ 求出 M_{ρ^2}，从而得到 ρ^2. 在进行关系矩阵的乘法运算时，矩阵中元素的相乘和相加均使用布尔运算.

$$M_\rho=\begin{array}{c}\\a\\b\\c\\d\end{array}\begin{array}{c}\begin{matrix}a&b&c&d\end{matrix}\\\begin{bmatrix}1&1&0&0\\0&0&0&1\\1&0&0&0\\0&0&1&0\end{bmatrix}\end{array},$$

$$M_{\rho^2}=M_\rho\cdot M_\rho=\begin{bmatrix}1&1&0&0\\0&0&0&1\\1&0&0&0\\0&0&1&0\end{bmatrix}\cdot\begin{bmatrix}1&1&0&0\\0&0&0&1\\1&0&0&0\\0&0&1&0\end{bmatrix}=\begin{array}{c}\\a\\b\\c\\d\end{array}\begin{array}{c}\begin{matrix}a&b&c&d\end{matrix}\\\begin{bmatrix}1&1&0&1\\0&0&1&0\\1&1&0&0\\1&0&0&0\end{bmatrix}\end{array}.$$

根据关系矩阵的表示方法，将矩阵M_{ρ^2}中为1的项转化为序偶，可以看到其结果与方法一完全相同.

方法三

构造出ρ的关系图，在图中从每一结点x出发，找出经过长为2的路能够到达的所有结点$y_1,y_2,\cdots,y_r$，于是在ρ^2的关系图中有r条边(x,y_1)、(x,y_2)、$\cdots$、(x,y_r).

本例ρ的关系图如图2-3所示. 从结点a出发，经过长为2的路可以到达的结点分别是a、b和d；从结点b出发，经过长为2的路可以到达的结点仅有c一个；从结点c出发，经过长为2的路可以到达的结点分别是a和b；从结点d出发，经过长为2的路仅可以到达结点a. 于是ρ^2的关系图的构造如图2-4所示.

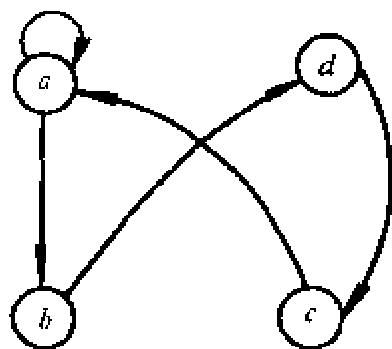


图2-3　ρ的关系图

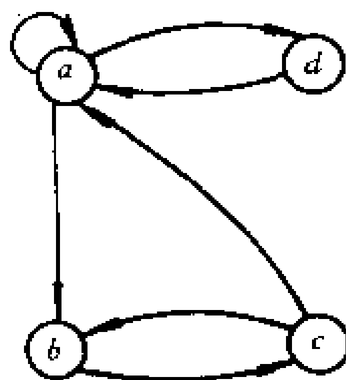


图2-4　ρ^2的关系图

根据ρ^2关系图中的边，写出相应的序偶，所得的结果与方法一完全相同.

例2-16　设有集合$A=\{2,3,4\}$，$B=\{4,6,7\}$，$C=\{8,9,12,14\}$，ρ_1是由A到B的关系，ρ_2是由B到C的关系，分别定义为

$$\rho_1=\{(a,b)\mid a\text{是素数且}a\text{整除}b\},$$

$$\rho_2=\{(b,c)\mid b\text{整除}c\};$$

试用关系矩阵表示法求复合关系$\rho_1\cdot\rho_2$.

解　$\rho_1=\{(2,4),(2,6),(3,6)\}$；

$\rho_2=\{(4,8),(4,12),(6,12),(7,14)\}$.

因此

$$M_{\rho_1}=\begin{matrix} & \begin{matrix}4 & 6 & 7\end{matrix} \\ \begin{matrix}2\\3\\4\end{matrix} & \begin{bmatrix}1 & 1 & 0\\0 & 1 & 0\\0 & 0 & 0\end{bmatrix}\end{matrix},\quad M_{\rho_2}=\begin{matrix} & \begin{matrix}8 & 9 & 12 & 14\end{matrix} \\ \begin{matrix}4\\6\\7\end{matrix} & \begin{bmatrix}1 & 0 & 1 & 0\\0 & 0 & 1 & 0\\0 & 0 & 0 & 1\end{bmatrix}\end{matrix},$$

$$M_{\rho_1\cdot\rho_2}=M_{\rho_1}\cdot M_{\rho_2}=\begin{bmatrix}1 & 1 & 0\\0 & 1 & 0\\0 & 0 & 0\end{bmatrix}\cdot\begin{bmatrix}1 & 0 & 1 & 0\\0 & 0 & 1 & 0\\0 & 0 & 0 & 1\end{bmatrix}$$

$$=\begin{matrix} & \begin{matrix}8 & 9 & 12 & 14\end{matrix} \\ \begin{matrix}2\\3\\4\end{matrix} & \begin{bmatrix}1 & 0 & 1 & 0\\0 & 0 & 1 & 0\\0 & 0 & 0 & 0\end{bmatrix}\end{matrix},$$

故 $$\rho_1\cdot\rho_2=\{(2,8),(2,12),(3,12)\}.$$

（3）关系的闭包运算

如前所述，如果 ρ 是定义在有限集 A 上的关系，则一定存在某个正整数 m，使得 ρ 的传递闭包 $\rho^+=\bigcup_{i=1}^{m}\rho^i$. 事实上可以证明，对于任意基数为 n 的有限集 A，A 上关系 ρ 的传递闭包

$$\rho^+=\bigcup_{i=1}^{n}\rho^i=\rho\cup\rho^2\cup\cdots\cup\rho^n,$$

即 ρ^+ 可表示为 A 上 n 个关系的并集，而这些关系中除 ρ 以外，其余均是复合关系，因此运用前面的方法可以求出 ρ^+. 下面介绍用关系图求 ρ^+ 的更简单的方法：构造出 ρ 的关系图，在图中从每一结点 x 出发，找出能够到达的所有结点，如 $y_1,y_2,\cdots,y_r$，则在 ρ^+ 的关系图中有边 $(x,y_1),(x,y_2),\cdots,(x,y_r)$.

例 2-17 用构造 ρ^+ 的关系图的方法，求例 2-10 中关系 ρ 的传递闭包 ρ^+.

解 （1）先构造出 ρ 的关系图（图 2-5）.

（2）在 ρ 的关系图中，对每一结点 x，找出从 x 出发能到达的所有结点. 从结点 a 出发可分别到达 a、b、c、e，从结点 b 出发可分

别到达结点 a,b,c,e，从结点 c 出发可到达结点 e，从结点 d 出发可分别到达 b、a、c、e.

(3) 构造 ρ^+ 的关系图(图 2-6).

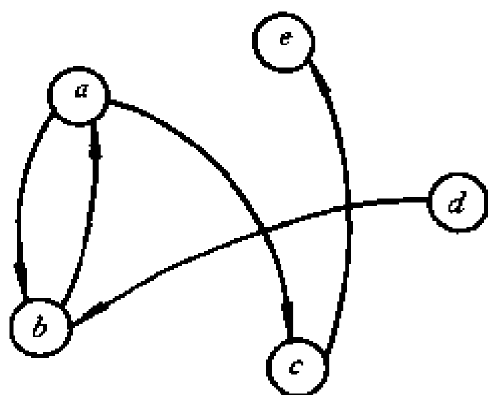


图 2-5 ρ 的关系图

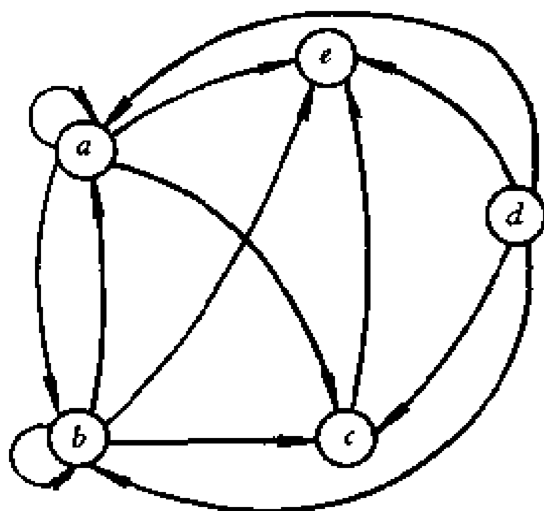


图 2-6 ρ^+ 的关系图

(4) 根据 ρ^+ 的关系图写出 ρ^+ 的相应序偶.

$$\rho^+=\{(a,a),(a,b),(a,c),(a,e),(b,a),(b,b),(b,c),(b,e),(c,e),(d,a),(d,b),(d,c),(d,e)\}.$$

12. 集合 A 上关系的性质

集合 A 上的关系可能具有各种不同的性质，根据它具有的不同性质，我们赋予它们相应不同的名称.

设 ρ 是集合 A 上的关系，若对于 A 中每一个元素 a，均有 $(a,a)\in\rho$，则称 ρ 是 A 上的自反关系；对于 A 中任意两个元素 a、b，若有 $(a,b)\in\rho$，则一定有 $(b,a)\in\rho$，即 (a,b) 和 (b,a) 或者同时出现于 ρ 中，或者均不在 ρ 中，这样的关系称为 A 上的对称关系；对于 A 中任意两个不同的元素 a,b，如果 (a,b) 和 (b,a) 至多只有一个在 ρ 中出现，则称 ρ 是 A 上的反对称关系；对于 A 中任意三个元素 a、b、c，若 ρ 中出现有 (a,b) 和 (b,c) 时，就一定出现 (a,c) 这个序偶，则称 ρ 是 A 上的可传递关系.

例 2-18 设 $A=\{a,b,c,d\}$.

(1) 判断下列关系是否自反关系.

$\rho_1=\{(a,b),(b,c)\}$;

$\rho_2=\{(a,a),(b,b),(c,c),(d,a)\}$;

$\rho_3=\{(a,a),(a,b),(d,d),(c,c),(b,b)\}$;

$\rho_4=\{(a,a),(b,b),(d,d),(c,c)\}$.

解 ρ_1 不是自反关系,因为对于所有的 $x\in A$,(x,x)均不在 ρ_1 中.

ρ_2 不是自反关系,因为$(d,d)\notin\rho_2$.

ρ_3 是自反关系,但不是恒等关系.

ρ_4 是自反关系,也是恒等关系.

(2) 判断下列关系是否对称关系或反对称关系.

$\rho_5=\{(a,b),(a,a),(b,a),(b,c),(c,b)\}$;

$\rho_6=\{(a,b),(a,a),(b,c),(d,c)\}$;

$\rho_7=\{(c,b),(a,a),(d,c),(c,d)\}$;

$\rho_8=\{(b,b),(d,d)\}$.

解 ρ_5 是对称关系. 它不是反对称关系,因为 $a\neq b$,但(a,b)和 (b,a)均出现在 ρ_5 中. 同样 $b\neq c$,但(b,c)和(c,b)均出现在 ρ_5 中.

ρ_6 不是对称关系,因为$(a,b)\in\rho_6$,但$(b,a)\notin\rho_6$. 同样$(b,c)\in\rho_6$,但$(c,b)\notin\rho_6$,$(d,c)\in\rho_6$ 但$(c,d)\notin\rho_6$. 而上述这几条原因正好说明 ρ_6 是反对称关系.

ρ_7 不是对称关系,因为$(c,b)\in\rho_7$ 但$(b,c)\notin\rho_7$. 它也不是反对称关系,因为 $c\neq d$,但(c,d)和(d,c)均在 ρ_7 中.

ρ_8 既是对称关系,也是反对称关系.

(3) 判断下列关系是否可传递的关系.

$\rho_9=\{(b,c),(c,c),(c,d),(b,d)\}$;

$\rho_{10}=\{(b,c),(c,b),(b,b),(a,d)\}$;

$\rho_{11}=\{(b,c),(d,a),(d,c)\}$.

解 ρ_9 是可传递的关系.

ρ_{10}不是可传递的关系. 因为$(c,b)\in\rho_{10}$,$(b,c)\in\rho_{10}$,但$(c,c)\notin\rho_{10}$.

ρ_{11}是可传递的关系. 在此例中没有出现$(x,y)\in\rho_{11}$同时$(y,z)\in\rho_{11}$的情形,因此也就无所谓$(x,z)\in\rho_{11}$的要求.

13. 构造传递闭包的又一种方法

我们知道,传递闭包 ρ^+ 具有以下三条性质:

(1) $\rho\subseteq\rho^+$;

(2) ρ^+是集合 A 上的可传递关系;

(3) 对于集合 A 上任意的可传递关系 ρ_t,若 $\rho\subseteq\rho_t$,则 $\rho^+\subseteq\rho_t$.

以上三条性质说明 ρ^+是集合 A 上所有包含 ρ 的可传递关系中最小的一个关系. 这三条性质可唯一地确定传递闭包 ρ^+. 也就是说,如果我们能构造一个满足上述条件(1)和(2),而又具有最少序偶的关系,那么该关系就是 ρ^+. 因此我们可以采用在 ρ 中添加序偶的方法来构造 ρ^+. 所添加的序偶必须是为了使得 ρ 具有可传递性而需要的.

例 2-19 设 $A=\{a,b,c,d\}$,ρ_1 和 ρ_2 是 A 上的关系

$$\rho_1=\{(d,c),(c,a),(b,b),(d,a)\},$$
$$\rho_2=\{(b,c),(c,d),(c,b)\},$$

试问 $\rho_1^+=?$,$\rho_2^+=?$

解 因为 $\rho_1\subseteq\rho_1$ 且 ρ_1 是可传递的,而 ρ_1 显然是满足(1),(2)这两条件中最小的关系,所以 $\rho_1^+=\rho_1$.

ρ_2 不是可传递的,因为有$(b,c)\in\rho_2$,$(c,d)\in\rho_2$,但$(b,d)\notin\rho_2$. 所以必须添加(b,d). 类似地道理,也必须添加(b,b)和(c,c).

注意到序偶(b,d),(b,b)和(c,c)是必须添加的,否则无法使 ρ_2 变成可传递关系. 而添加了这三个序偶后,ρ_2 变成可传递了,因此不能再添加其它的序偶,故

$\rho_2^+ = \{(b,c),(c,d),(c,b),(b,d),(b,b),(c,c)\}$.

14. 等价关系

(1) 等价关系

若 ρ 是集合 A 上的关系，而且 ρ 同时具有自反性、对称性和可传递性，那么称 ρ 是 A 上的等价关系.

例 2-20 设 $A=\{a,b,c,d,e\}$，A 上的关系

$\rho_1=\{(a,a),(b,a),(b,b),(d,e),(a,b),(e,d),(d,d),(c,c),(e,e)\}$，

$\rho_2=\{(b,b),(b,a),(a,b),(d,d),(d,e),(c,c)\}$，

试判断 ρ_1 和 ρ_2 是否等价关系.

解 ρ_1 是等价关系. 因为它具有自反性、对称性和可传递性.

ρ_2 不是等价关系. 原因是：1) $(a,a)\notin\rho_2$，$(e,e)\notin\rho_2$，所以 ρ_2 不具有自反性；2) $(d,e)\in\rho_2$，但 $(e,d)\notin\rho_2$，所以 ρ_2 不具有对称性；3) $(a,b)\in\rho_2$，$(b,a)\in\rho_2$，但 $(a,a)\notin\rho_2$，所以 ρ_2 不具有可传递性.

虽然有以上三条原因，然而其中单独任何一条均可使得 ρ_2 不成为等价关系. 例如

$\rho_3=\{(b,a),(a,b),(b,e),(a,c),(b,b),(a,a),(e,b),(c,a),(c,c),(d,d),(e,e)\}$

是 A 上的自反且对称的关系，但因 ρ_3 不是可传递的，所以 ρ_3 不是等价关系.

(2) 等价类

设 ρ 是集合 A 上的等价关系，若 $(a,b)\in\rho$，则称 a 与 b 等价. 由于 ρ 的对称性，也必有 $(b,a)\in\rho$，因此 b 也与 a 等价.

我们将集合 A 中所有与元素 a 等价的元素所构成的集合，称为元素 a 生成的等价类，用符号 $[a]_\rho$ 表示. 显然集合 A 中每一个元素均可生成一个等价类.

例 2-21 试对例 2-20 中等价关系 ρ_1 写出集合 A 中每一个元素生成的等价类.

解 对于元素 a,因为$(a,a)\in\rho_1$,$(b,a)\in\rho_1$,所以 a 生成的等价类$[a]_{\rho_1}=\{a,b\}$.

对于元素 b,因为$(b,b)\in\rho_1$,$(a,b)\in\rho_1$,所以 b 生成的等价类$[b]_{\rho_1}=\{a,b\}$.

类似地,$[c]_{\rho_1}=\{c\}$,$[d]_{\rho_1}=\{e,d\}$,$[e]_{\rho_1}=\{e,d\}$.

由上看出$[a]_{\rho_1}=[b]_{\rho_1}$,$[d]_{\rho_1}=[e]_{\rho_1}$,这说明不同的元素可能生成的等价类是相同的.

(3) 等价分划

由于等价关系具有对称性和可传递性,因此,如果集合 A 中元素 x 与 y 等价,那么 A 中凡是与 y 等价的元素必与 x 等价,反之,凡是与 x 等价的元素必与 y 等价. 因此必有$[x]_\rho=[y]_\rho$.

如果 x 与 y 不等价,则不但$[x]_\rho\neq[y]_\rho$,而且$[x]_\rho\cap[y]_\rho=\varnothing$,即没有元素能够既与 x 等价,又与 y 等价. 因此 A 中元素产生的所有等价类构成 A 的一个分划,称作是等价分划. 记作 Π_ρ^A.

例如,上例中集合 A 上由 ρ_1 导出的等价分划是

$$\Pi_{\rho_1}^A=\{\{a,b\},\{c\},\{d,e\}\}=\{[a]_{\rho_1},[c]_{\rho_1},[d]_{\rho_1}\}.$$

15. 偏序关系

若 ρ 是集合 A 上的关系,而且 ρ 同时具有自反性、反对称性和可传递性,那么称 ρ 是 A 上的偏序关系. 偏序关系常特定地用符号“$\leqslant$”表示.

例 2-22 设 $A=\{2,3,4,6,8\}$,ρ 是 A 上的关系,定义为

$$\rho=\{(a,b)\mid a\text{ 整除 }b\}.$$

试问 ρ 是偏序关系吗?

解 由 ρ 的定义,ρ 由以下序偶组成

$$\rho=\{(2,2),(2,4),(2,6),(2,8),(3,3),(3,6),(4,4),(4,8),(6,6),(8,8)\}.$$

因为$(2,2)$,$(3,3)$,$(4,4)$,$(6,6)$,$(8,8)$均在 ρ 中,所以 ρ 是自反的.

当 $a \neq b$ 时，序偶(a,b)和(b,a)至多只有一个在 ρ 中，所以 ρ 是反对称的.

检查每一对序偶可以看出，每当有(a,b)，$(b,c) \in \rho$ 时，便有$(a,c) \in \rho$. 例如$(2,4)$，$(4,8) \in \rho$，也有$(2,8) \in \rho$. 所以 ρ 是可传递的.

由上可知 ρ 是 A 上的偏序关系.

事实上，只要 A 是由一些正整数组成的集合，则 A 上的整除关系一定是偏序关系.

对于有限集 A 上的偏序关系，既可以用关系图表示，也可以用次序图表示. 用次序图表示比用关系图表示简洁得多.

例 2-23 分别用关系图和次序图表示例 2-22 中的偏序关系 ρ.

解 偏序关系 ρ 的关系图和次序图分别如图 2-7 和图 2-8 所示.

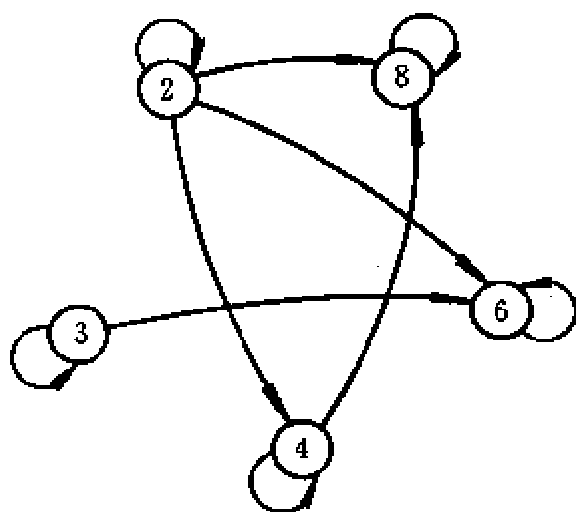


图 2-7 ρ 的关系图

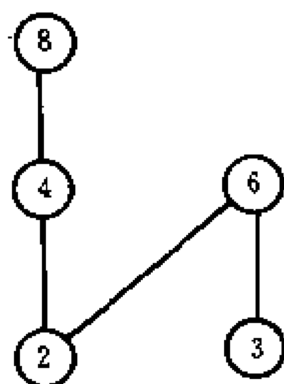


图 2-8 ρ 的次序图

偏序关系又称为部分序关系，它使得集合 A 中部分元素之间呈现一种次序关系. 这种次序关系在关系图中体现不出来，但在次序图中却表现得很清楚.

如上例中 $2 \leqslant 4 \leqslant 8$，$3 \leqslant 6$，$2 \leqslant 6$. 而 4 与 6 之间，6 与 8 之间没

有这种次序关系，因为它们相互都不能整除对方.

2.3 问答与论证

例 2-24 设 A、B、C 和 D 是任意的集合，试问下列等式是否成立？为什么？

(1) $(A\cap B)\times(C\cap D)=(A\times C)\cap(B\times D)$；

(2) $(A\cup B)\times(C\cup D)=(A\times C)\cup(B\times D)$.

解 (1) 成立. 可以通过证明

$$(A\cap B)\times(C\cap D)\subseteq(A\times C)\cap(B\times D)$$

和

$$(A\times C)\cap(B\times D)\subseteq(A\cap B)\times(C\cap D)$$

来证明这一等式成立.

首先，因为 $A\cap B\subseteq A, C\cap D\subseteq C$，所以

$$(A\cap B)\times(C\cap D)\subseteq A\times C.$$

类似地 $A\cap B\subseteq B, C\cap D\subseteq D$，所以

$$(A\cap B)\times(C\cap D)\subseteq B\times D,$$

$$(A\cap B)\times(C\cap D)\subseteq(A\times C)\cap(B\times D).$$

反之，若$(x,y)\in(A\times C)\cap(B\times D)$，则

$$(x,y)\in A\times C \text{ 且} (x,y)\in B\times D,$$

因此 $x\in A, y\in C$ 且 $x\in B, y\in D$. 于是

$$x\in A\cap B, y\in C\cap D,$$

因而$(x,y)\in(A\cap B)\times(C\cap D)$，故

$$(A\times C)\cap(B\times D)\subseteq(A\cap B)\times(C\cap D).$$

由上可知$(A\cap B)\times(C\cap D)=(A\times C)\cap(B\times D)$.

(2) 不成立. 其分析如下：

∵ $A\subseteq A\cup B, C\subseteq C\cup D$,

∴ $(A\times C)\subseteq(A\cup B)\times(C\cup D)$.

类似地$(B\times D)\subseteq(A\cup B)\times(C\cup D)$. 因此

$$(A \times C) \cup (B \times D) \subseteq (A \cup B) \times (C \cup D).$$

但是$(A\cup B)\times(C\cup D)\subseteq(A\times C)\cup(B\times D)$却不成立，因为，若$(x,y)\in(A\cup B)\times(C\cup D)$，则$x\in A\cup B, y\in C\cup D$，此时可能$x\in A$而$x\notin B, y\in D$而$y\notin C$，于是

$$(x,y) \notin A \times C \quad \text{且} (x,y) \notin B \times D,$$

因而
$$(x,y) \notin (A \times C) \cup (B \times D).$$

例如，设$A=\{a\}, B=\{b\}, C=\{c\}, D=\{d\}$，则

$$A \cup B = \{a,b\}, C \cup D = \{c,d\}.$$

显然$(a,d)\in(A\cup B)\times(C\cup D)$，但

$$(a,d) \notin A \times C \text{且} (a,d) \notin B \times D,$$

因此$(a,d)\notin(A\times C)\cup(B\times D)$.

由此可知，对于任意的集合A、B、C和D，(2)式不成立.

例 2-25 设ρ_1和ρ_2是由A到B的任意两个关系，试证明$D_{\rho_1\cup\rho_2}=D_{\rho_1}\cup D_{\rho_2}$. 等式$R_{\rho_1\cap\rho_2}=R_{\rho_1}\cap R_{\rho_2}$成立吗？为什么？

证 设$a\in D_{\rho_1\cup\rho_2}$，则必存在$b\in B$，使得$(a,b)\in\rho_1\cup\rho_2$，于是$(a,b)\in\rho_1$或$(a,b)\in\rho_2$，因此$a\in D_{\rho_1}$或$a\in D_{\rho_2}$，即$a\in D_{\rho_1}\cup D_{\rho_2}$，故$D_{\rho_1\cup\rho_2}\subseteq D_{\rho_1}\cup D_{\rho_2}$.

反之，设$a\in D_{\rho_1}\cup D_{\rho_2}$，则$a\in D_{\rho_1}$或$a\in D_{\rho_2}$，于是存在$b_1\in B$，使$(a,b_1)\in\rho_1$，或者存在$b_2\in B$，使$(a,b_2)\in\rho_2$，由并集的定义有$(a,b_1)\in\rho_1\cup\rho_2$或者$(a,b_2)\in\rho_1\cup\rho_2$，总之有$a\in D_{\rho_1\cup\rho_2}$，故$D_{\rho_1}\cup D_{\rho_2}\subseteq D_{\rho_1\cup\rho_2}$.

由上可知$D_{\rho_1\cup\rho_2}=D_{\rho_1}\cup D_{\rho_2}$.

等式$R_{\rho_1\cap\rho_2}=R_{\rho_1}\cap R_{\rho_2}$不成立.

我们可以证明$R_{\rho_1\cap\rho_2}\subseteq R_{\rho_1}\cap R_{\rho_2}$是成立的.

设$b\in R_{\rho_1\cap\rho_2}$，则必存在$a\in A$，使$(a,b)\in\rho_1\cap\rho_2$，于是$(a,b)\in\rho_1$且$(a,b)\in\rho_2$，因此$b\in R_{\rho_1}$且$b\in R_{\rho_2}$，由交集的定义$b\in R_{\rho_1}\cap R_{\rho_2}$，故$R_{\rho_1\cap\rho_2}\subseteq R_{\rho_1}\cap R_{\rho_2}$.

但$R_{\rho_1}\cap R_{\rho_2}\nsubseteq R_{\rho_1\cap\rho_2}$. 下面证明包含关系成立，看会遇到什么

问题.

设 $b\in R_{\rho_1}\cap R_{\rho_2}$，则 $b\in R_{\rho_1}$ 且 $b\in R_{\rho_2}$，由

$b\in R_{\rho_1}$，必存在 $a_1\in A$，使得 $(a_1,b)\in\rho_1$，

$b\in R_{\rho_2}$，必存在 $a_2\in A$，使得 $(a_2,b)\in\rho_2$.

在这里 a_1 是否等于 a_2，我们无法知道，因此必须用两个不同的符号表示. 事实上可能不存在公共的元素 $a\in A$，使得 $(a,b)\in\rho_1$ 且 $(a,b)\in\rho_2$，因此也就不存在元素 $a\in A$，使得 $(a,b)\in\rho_1\cap\rho_2$，因而无法推出 $b\in R_{\rho_1\cap\rho_2}$.

反例如下：

设 $A=\{1,2,3\}$，$B=\{2,4,5\}$，

$\rho_1=\{(1,2),(1,4)\}$，$\rho_2=\{(3,2),(1,4),(3,5)\}$，

则
$$\rho_1\cap\rho_2=\{(1,4)\}.$$
于是 $R_{\rho_1}=\{2,4\}$，$R_{\rho_2}=\{2,4,5\}$，因此
$$R_{\rho_1}\cap R_{\rho_2}=\{2,4\},$$
而 $R_{\rho_1\cap\rho_2}=\{4\}$，所以
$$R_{\rho_1}\cap R_{\rho_2}\not\subseteq R_{\rho_1\cap\rho_2}.$$

注意在此例中有 $(1,2)\in\rho_1$，$(3,2)\in\rho_2$，因此 $2\in R_{\rho_1}$，$2\in R_{\rho_2}$，但不存在任何元素 $a\in A$，使 $(a,2)\in\rho_1\cap\rho_2$，所以 $2\notin R_{\rho_1\cap\rho_2}$.

例 2-26 设 ρ_1 是由集合 A 到 B 的关系，ρ_2 是由 B 到 C 的关系. 试证明 $\widetilde{\rho_1\cdot\rho_2}=\tilde{\rho}_2\cdot\tilde{\rho}_1$.

证 由题设 $\widetilde{\rho_1\cdot\rho_2}$ 和 $\tilde{\rho}_2\cdot\tilde{\rho}_1$ 均是由 C 到 A 的关系，因此只要证明它们由完全相同的序偶所组成.

设 $(c,a)\in\widetilde{\rho_1\cdot\rho_2}$，则 $(a,c)\in\rho_1\cdot\rho_2$，因此必存在元素 $b\in B$，使得 $(a,b)\in\rho_1$，$(b,c)\in\rho_2$，于是 $(c,b)\in\tilde{\rho}_2$，$(b,a)\in\tilde{\rho}_1$，因此 $(c,a)\in\tilde{\rho}_2\cdot\tilde{\rho}_1$，故 $\widetilde{\rho_1\cdot\rho_2}\subseteq\tilde{\rho}_2\cdot\tilde{\rho}_1$.

反之，设 $(c,a)\in\tilde{\rho}_2\cdot\tilde{\rho}_1$，则必存在元素 $b'\in B$，使得 $(c,b')\in\tilde{\rho}_2$，$(b',a)\in\tilde{\rho}_1$，于是 $(a,b')\in\rho_1$，$(b',c)\in\rho_2$，因此 $(a,c)\in\rho_1\cdot\rho_2$，

于是$(c,a)\in\widetilde{\rho_1\cdot\rho_2}$，故$\tilde{\rho}_2\cdot\tilde{\rho}_1\subseteq\widetilde{\rho_1\cdot\rho_2}$.

由上证得 $\widetilde{\rho_1\cdot\rho_2}=\tilde{\rho}_2\cdot\tilde{\rho}_1$.

例 2-27 设 A 是具有 n 个元素的有限集，ρ 是 A 上的关系. 试证明必存在两个正整数 k 和 t，使得 $\rho^k=\rho^t$.

证 因为 ρ 是 A 上的关系，所以对于任意正整数 r，ρ^r 也都是 A 上的关系. 另一方面，因为 $\# A=n$，所以 $\#(A\times A)=n^2$，$\#(2^{A\times A})=2^{\#(A\times A)}=2^{n^2}$，这意味着 A 上只有 2^{n^2} 个不同的关系，因此在关系

$$\rho,\rho^2,\rho^3,\cdots,\rho^{2^{n^2}},\rho^{2^{n^2}+1}$$

中必有两个是相同的. 即存在正整数 k 和 t，$1\leqslant k<t\leqslant 2^{n^2}+1$，使得 $\rho^k=\rho^t$.

例 2-28 设 ρ_1 是由 A 到 B 的关系，ρ_2 和 ρ_3 是由 B 到 C 的关系. 试证明

(1) $\rho_1\cdot(\rho_2\cup\rho_3)=\rho_1\cdot\rho_2\cup\rho_1\cdot\rho_3$；

(2) $\rho_1\cdot(\rho_2\cap\rho_3)\subseteq\rho_1\cdot\rho_2\cap\rho_1\cdot\rho_3$.

又 (3) $\rho_1\cdot\rho_2\cap\rho_1\cdot\rho_3\subseteq\rho_1\cdot(\rho_2\cap\rho_3)$成立否？为什么？

证 (1) 根据并集和复合关系的定义，$\rho_1\cdot(\rho_2\cup\rho_3)$和 $\rho_1\cdot\rho_2\cup\rho_1\cdot\rho_3$ 都是由 A 到 C 的关系. 因此只要证明它们由完全相同的序偶所组成.

设$(a,c)\in\rho_1\cdot(\rho_2\cup\rho_3)$，则必存在 $b\in B$，使得$(a,b)\in\rho_1$，$(b,c)\in\rho_2\cup\rho_3$，于是$(b,c)\in\rho_2$ 或$(b,c)\in\rho_3$，因此$(a,c)\in\rho_1\cdot\rho_2$，或$(a,c)\in\rho_1\cdot\rho_3$，于是$(a,c)\in\rho_1\cdot\rho_2\cup\rho_1\cdot\rho_3$，故

$$\rho_1\cdot(\rho_2\cup\rho_3)\subseteq\rho_1\cdot\rho_2\cup\rho_1\cdot\rho_3.$$

反之，设$(a,c)\in\rho_1\cdot\rho_2\cup\rho_1\cdot\rho_3$，则$(a,c)\in\rho_1\cdot\rho_2$ 或$(a,c)\in\rho_1\cdot\rho_3$，若$(a,c)\in\rho_1\cdot\rho_2$，则存在 $b_1\in B$，使得$(a,b_1)\in\rho_1$，$(b_1,c)\in\rho_2$，于是有$(a,b_1)\in\rho_1$，$(b_1,c)\in\rho_2\cup\rho_3$，因此$(a,c)\in\rho_1\cdot(\rho_2\cup\rho_3)$；若$(a,c)\in\rho_1\cdot\rho_3$，则存在 $b_2\in B$，使得$(a,b_2)\in\rho_1$，$(b_2,c)\in\rho_3$，类似地有$(a,c)\in\rho_1\cdot(\rho_2\cup\rho_3)$，故 $\rho_1\cdot\rho_2\cup\rho_1\cdot\rho_3\subseteq\rho_1\cdot(\rho_2\cup\rho_3)$.

由上证得 $\rho_1 \cdot (\rho_2 \cup \rho_3) = \rho_1 \cdot \rho_2 \cup \rho_1 \cdot \rho_3$.

（2）设 $(a,c) \in \rho_1 \cdot (\rho_2 \cap \rho_3)$，则存在 $b \in B$，使得 $(a,b) \in \rho_1$，$(b,c) \in \rho_2 \cap \rho_3$，因此 $(b,c) \in \rho_2$ 且 $(b,c) \in \rho_3$，于是 $(a,c) \in \rho_1 \cdot \rho_2$，且 $(a,c) \in \rho_1 \cdot \rho_3$，因此 $(a,c) \in \rho_1 \cdot \rho_2 \cap \rho_1 \cdot \rho_3$. 故 $\rho_1 \cdot (\rho_2 \cap \rho_3) \subseteq \rho_1 \cdot \rho_2 \cap \rho_1 \cdot \rho_3$.

解　(3) $\rho_1 \cdot \rho_2 \cap \rho_1 \cdot \rho_3 \subseteq \rho_1 \cdot (\rho_2 \cap \rho_3)$ 不成立. 分析如下：

若设 $(a,c) \in \rho_1 \cdot \rho_2 \cap \rho_1 \cdot \rho_3$，则 $(a,c) \in \rho_1 \cdot \rho_2$ 且 $(a,c) \in \rho_1 \cdot \rho_3$，因此，必存在 $b_1 \in B$，使 $(a,b_1) \in \rho_1$，$(b_1,c) \in \rho_2$；

必存在 $b_2 \in B$，使 $(a,b_2) \in \rho_1$，$(b_2,c) \in \rho_3$.

在这里 b_1 与 b_2 很可能是两个不同的元素，甚至不存在 $b_1 = b_2$ 的可能性. 因此在这种情形下，要想推出 $(a,c) \in \rho_1 \cdot (\rho_2 \cap \rho_3)$ 是不可能. 因为 $(a,c) \in \rho_1 \cdot (\rho_2 \cap \rho_3)$ 意味着存在一个公共元素 $b \in B$，使得 $(a,b) \in \rho_1$，$(b,c) \in \rho_2$ 且 $(b,c) \in \rho_3$.

反例如下：

设 $A = \{a,b,c\}$，$B = \{d,e,f\}$，$C = \{1,2,3\}$，$\rho_1 = \{(a,d),(a,e),(a,f)\}$，$\rho_2 = \{(d,1),(f,3)\}$，$\rho_3 = \{(d,1),(e,3)\}$.

则　　$\rho_2 \cap \rho_3 = \{(d,1)\}$，$\rho_1 \cdot (\rho_2 \cap \rho_3) = \{(a,1)\}$，

但　　$\rho_1 \cdot \rho_2 = \{(a,1),(a,3)\}$，$\rho_1 \cdot \rho_3 = \{(a,1),(a,3)\}$.

于是 $\rho_1 \cdot \rho_2 \cap \rho_1 \cdot \rho_3 = \{(a,1),(a,3)\}$，因此

$$\rho_1 \cdot \rho_2 \cap \rho_1 \cdot \rho_3 \nsubseteq \rho_1 \cdot (\rho_2 \cap \rho_3)$$

注意到 $(a,3) \in \rho_1 \cdot \rho_2 \cap \rho_1 \cdot \rho_3$，但 $(a,3) \notin \rho_1 \cdot (\rho_2 \cap \rho_3)$，原因是不存在一个公共的元素 $x \in B$，能使 $(x,3) \in \rho_2$，且 $(x,3) \in \rho_3$.

例 2-29　设 ρ 是基数为 n 的集合 A 上的一个关系. 试证明 ρ 的传递闭包 $\rho^+ = \bigcup_{i=1}^{n} \rho^i$.

分析　由定义 $\rho^+ = \bigcup_{i=1}^{\infty} \rho^i$，要证明 $\rho^+ = \bigcup_{i=1}^{n} \rho^i$，即要证明 $\bigcup_{i=1}^{\infty} \rho^i = \bigcup_{i=1}^{n} \rho^i$. 显然 $\bigcup_{i=1}^{n} \rho^i \subseteq \bigcup_{i=1}^{\infty} \rho^i$，因此只要证明 $\bigcup_{i=1}^{\infty} \rho^i \subseteq \bigcup_{i=1}^{n} \rho^i$ 即可.

证　设 $(a,b) \in \bigcup_{i=1}^{\infty} \rho^i$，则必存在正整数 k，使得 $(a,b) \in \rho^k$.

若 $k\leqslant n$，则 $(a,b)\in\bigcup_{i=1}^{n}\rho^i$.

若 $k>n$，则在 A 中必存在 $k-1$ 个元素 $a_{i_1},a_{i_2},\cdots,a_{i_{k-1}}$，使得

$$a\rho a_{i_1},a_{i_1}\rho a_{i_2},\cdots,a_{i_{k-1}}\rho b.$$

因为 $k>n$，所以在 $a,a_{i_1},a_{i_2},\cdots,a_{i_{k-1}},b$ 这 $k+1$ 个元素中必有两个元素 $a_{i_r}=a_{i_t}(0\leqslant r<t\leqslant k$，记 a 为 a_{i_0}，记 b 为 $a_{i_k})$，因此下述关系

$$a\rho a_{i_1},\cdots,a_{i_{r-1}}\rho a_{i_r},a_{i_t}\rho a_{i_{t+1}},\cdots,a_{i_{k-1}}\rho b$$

成立. 这表明 $a\rho^{k_1}b,k_1=k-(t-r),k_1<k$.

若 $k_1>n$，用类似的方法又可找到 $k_2<k_1$，使 $a\rho^{k_2}b,\cdots$，最后必可找到一正整数 h，使 $a\rho^h b$，且 $h\leqslant n$. 因此 $(a,b)\in\bigcup_{i=1}^{n}\rho^i$. 故 $\bigcup_{i=1}^{\infty}\rho^i\subseteq\bigcup_{i=1}^{n}\rho^i$.

由上可知 $\rho^+=\bigcup_{i=1}^{n}\rho^i$.

例 2-30 设 ρ_1 和 ρ_2 是集合 A 上的两个关系，试证明 $\rho_1^+\cup\rho_2^+\subseteq(\rho_1\cup\rho_2)^+$. 又 $(\rho_1\cup\rho_2)^+\subseteq\rho_1^+\cup\rho_2^+$ 成立吗？为什么？

证

证法一(根据 ρ^+ 的定义进行推理)

设 $(a,b)\in\rho_1^+\cup\rho_2^+$，则 $(a,b)\in\rho_1^+$ 或 $(a,b)\in\rho_2^+$.

若 $(a,b)\in\rho_1^+$，则必存在正整数 k，使得 $(a,b)\in\rho_1^k$，于是存在元素 $a_{i_1},a_{i_2},\cdots,a_{i_{k-1}}\in A$，使得

$$a\rho_1 a_{i_1},a_{i_1}\rho_1 a_{i_2},\cdots,a_{i_{k-1}}\rho_1 b.$$

因为 $\rho_1\subseteq\rho_1\cup\rho_2$，所以又有

$$a(\rho_1\cup\rho_2)a_{i_1},a_{i_1}(\rho_1\cup\rho_2)a_{i_2},\cdots,a_{i_{k-1}}(\rho_1\cup\rho_2)b,$$

于是 $\qquad a(\rho_1\cup\rho_2)^k b$，即 $(a,b)\in(\rho_1\cup\rho_2)^k$，

由 $\quad(\rho_1\cup\rho_2)^k\subseteq(\rho_1\cup\rho_2)^+$，因此

$$(a,b)\in(\rho_1\cup\rho_2)^+.$$

若 $(a,b)\in\rho_2^+$，类似地可以证明 $(a,b)\in(\rho_1\cup\rho_2)^+$. 由 (a,b) 的任意性，可得 $\rho_1^+\cup\rho_2^+\subseteq(\rho_1\cup\rho_2)^+$.

证法二(根据 ρ^+ 的性质进行推理)

由 ρ^+ 的定义,$\rho^+=\bigcup_{i=1}^{\infty}\rho^i=\rho\cup\rho^2\cup\rho^3\cup\cdots$,因此

$$\rho_1\subseteq\rho_1^+,\text{又 }\rho_1\subseteq\rho_1\cup\rho_2\subseteq(\rho_1\cup\rho_2)^+$$

根据传递闭包的性质,ρ_1^+ 包含于每一个包含 ρ_1 的可传递关系中,由于 $(\rho_1\cup\rho_2)^+$ 是 A 上包含 ρ_1 的可传递关系,所以 $\rho_1^+\subseteq(\rho_1\cup\rho_2)^+$.

类似地可以证明 $\rho_2^+\subseteq(\rho_1\cup\rho_2)^+$.

因此 $$\rho_1^+\cup\rho_2^+\subseteq(\rho_1\cup\rho_2)^-.$$

又 $(\rho_1\cup\rho_2)^+\subseteq\rho_1^+\cup\rho_2^+$ 不成立.可举反例如下:

设 $A=\{1,2,3\}$,A 上的关系 $\rho_1=\{(1,2)\}$,$\rho_2=\{(2,3)\}$

则 $\rho_1^+=\{(1,2)\}$,$\rho_2^+=\{(2,3)\}$,于是

$$\rho_1^+\cup\rho_2^+=\{(1,2),(2,3)\}$$

而 $(\rho_1\cup\rho_2)^+=\{(1,2),(2,3),(1,3)\}$,显然

$$(\rho_1\cup\rho_2)^+\nsubseteq\rho_1^+\cup\rho_2^+.$$

例 2-31 设 ρ_1 和 ρ_2 是集合 A 上的两个关系,判断下列命题是否正确.

(1) 若 ρ_1 和 ρ_2 是自反的,则 $\rho_1\cdot\rho_2$ 也是自反的;

(2) 若 ρ_1 和 ρ_2 是对称的,则 $\rho_1\cdot\rho_2$ 也是对称的;

(3) 若 ρ_1 和 ρ_2 是反对称的,则 $\rho_1\cdot\rho_2$ 也是反对称的;

(4) 若 ρ_1 和 ρ_2 是可传递的,则 $\rho_1\cdot\rho_2$ 也是可传递的.

解 (1) 命题显然正确.

因为 ρ_1 和 ρ_2 是自反的,所以对于任意的 $a\in A$,均有 $a\rho_1a$ 和 $a\rho_2a$.于是由复合关系的定义,对于任意的 $a\in A$,有 $a(\rho_1\cdot\rho_2)a$,因此 $\rho_1\cdot\rho_2$ 也是自反的.

(2) 命题错误.举反例如下:

设 $A=\{1,2,3\}$,A 上的关系

$$\rho_1=\{(1,2),(2,1)\},\rho_2=\{(1,3),(3,1)\}.$$

显然都是对称的.但 $\rho_1\cdot\rho_2=\{(2,3)\}$ 却不是对称的.

(3) 命题错误. 举反例如下：

设 $A=\{1,2,3\}$，A 上的关系

$$\rho_1=\{(1,2),(3,3)\},\rho_2=\{(2,3),(3,1)\}.$$

显然都是反对称的. 但 $\rho_1\cdot\rho_2=\{(1,3),(3,1)\}$ 却不是反对称的.

(4) 命题错误. 举反例如下：

设 $A=\{1,2,3\}$，A 上的关系

$$\rho_1=\{(1,2),(2,3),(1,3)\},\rho_2=\{(2,3),(3,1),(2,1)\}.$$

显然都是可传递的. 但 $\rho_1\cdot\rho_2=\{(1,3),(1,1),(2,1)\}$ 却不是可传递的.

例 2-32 设 ρ_1 是集合 A 上的一个关系，$\rho_2=\{(a,b)\mid$ 存在 c，使 $(a,c)\in\rho_1$ 且 $(c,b)\in\rho_1\}$. 试证明：若 ρ_1 是一个等价关系，则 ρ_2 也是一个等价关系.

证 证法一(根据等价关系的定义，证明 ρ_2 具有自反性、对称性和可传递性)

因为 ρ_1 是自反的，所以对于任意的 $a\in A$，有 $(a,a)\in\rho_1$. 由 $(a,a)\in\rho_1$，$(a,a)\in\rho_1$，因此有 $(a,a)\in\rho_2$，故 ρ_2 是自反的.

对于任意的 $a,b\in A$，若 $(a,b)\in\rho_2$，则必有元素 $c\in A$，使得 $(a,c)\in\rho_1$ 且 $(c,b)\in\rho_1$，由 ρ_1 的对称性又有 $(b,c)\in\rho_1$ 且 $(c,a)\in\rho_1$，因而有 $(b,a)\in\rho_2$，故 ρ_2 是对称的.

对于任意的 $a,b,c\in A$，若 $(a,b)\in\rho_2$，$(b,c)\in\rho_2$，则必有元素 $d,e\in A$，使得

$$(a,d)\in\rho_1,\quad (d,b)\in\rho_1;$$
$$(b,e)\in\rho_1,\quad (e,c)\in\rho_1.$$

由 ρ_1 的可传递性，又有 $(a,b)\in\rho_1$，$(b,c)\in\rho_1$，于是又有 $(a,c)\in\rho_2$，故 ρ_2 是可传递的.

由上证得 ρ_2 是一个等价关系.

证法二(通过证明 $\rho_2=\rho_1$，得到 ρ_2 是等价关系的结论)

设 $(a,b)\in\rho_1$，由 ρ_1 的自反性，又有 $(a,a)\in\rho_1$，由 $(a,a)\in\rho_1$，$(a,b)\in\rho_1$，于是有 $(a,b)\in\rho_2$，因此 $\rho_1\subseteq\rho_2$.

反之，设$(a,b)\in\rho_2$，则必存在$c\in A$，使得$(a,c)\in\rho_1$，$(c,b)\in\rho_1$，而由ρ_1的可传递性，又有$(a,b)\in\rho_1$，因此$\rho_2\subseteq\rho_1$.

由上可知$\rho_2=\rho_1$. 因此ρ_2是等价关系.

例 2-33 设ρ_1和ρ_2都是集合A上的等价关系. 试证明$\rho_1\cap\rho_2$也是A上的等价关系. $\rho_1\cup\rho_2$是A上的等价关系吗？为什么？

证 由交集的定义$\rho_1\cap\rho_2=\{(a,b)\mid(a,b)\in\rho_1\text{ 且}(a,b)\in\rho_2\}$.

对于任一$a\in A$，因为ρ_1和ρ_2都是自反的，所以有$(a,a)\in\rho_1$且$(a,a)\in\rho_2$，因而有$(a,a)\in\rho_1\cap\rho_2$，故$\rho_1\cap\rho_2$是自反的.

对于任意$a,b\in A$，若$(a,b)\in\rho_1\cap\rho_2$，则有$(a,b)\in\rho_1$且$(a,b)\in\rho_2$，由ρ_1和ρ_2的对称性有$(b,a)\in\rho_1$且$(b,a)\in\rho_2$，因而有$(b,a)\in\rho_1\cap\rho_2$，故$\rho_1\cap\rho_2$是对称的.

对于任意的$a,b,c\in A$，若$(a,b)\in\rho_1\cap\rho_2$，$(b,c)\in\rho_1\cap\rho_2$，则有$(a,b)\in\rho_1$，$(b,c)\in\rho_1$；$(a,b)\in\rho_2$，$(b,c)\in\rho_2$. 由ρ_1和ρ_2的可传递性有$(a,c)\in\rho_1$，$(a,c)\in\rho_2$，因而有$(a,c)\in\rho_1\cap\rho_2$，故$\rho_1\cap\rho_2$是可传递的.

由上证得$\rho_1\cap\rho_2$是A上的等价关系.

为了判断$\rho_1\cup\rho_2$是否A上的等价关系，我们试图来证明它的自反性、对称性和可传递性.

由并集的定义，$\rho_1\cup\rho_2=\{(a,b)\mid(a,b)\in\rho_1\text{ 或}(a,b)\in\rho_2\}$.

对于任一$a\in A$，因为ρ_1是自反的，所以有$(a,a)\in\rho_1$，因而有$(a,a)\in\rho_1\cup\rho_2$，故$\rho_1\cup\rho_2$是自反的.

对于任意的$a,b\in A$，若$(a,b)\in\rho_1\cup\rho_2$，则$(a,b)\in\rho_1$或$(a,b)\in\rho_2$，由于ρ_1和ρ_2都是对称的，因此又有$(b,a)\in\rho_1$或$(b,a)\in\rho_2$，因而有$(b,a)\in\rho_1\cup\rho_2$，故$\rho_1\cup\rho_2$是对称的.

对于任意的a、b、$c\in A$，若$(a,b)\in\rho_1\cup\rho_2$，$(b,c)\in\rho_1\cup\rho_2$，则

$$(a,b)\in\rho_1\quad\text{或}\quad(a,b)\in\rho_2;$$
$$(b,c)\in\rho_1\quad\text{或}\quad(b,c)\in\rho_2.$$

因为(a,b)和(b,c)不一定能同时属于ρ_1，也不一定能同时属于ρ_2，

所以我们无法推出$(a,c)\in\rho_1$或$(a,c)\in\rho_2$.因而也就无法推出$(a,c)\in\rho_1\cup\rho_2$.这说明$\rho_1\cup\rho_2$的可传递性不一定能成立，因此推不出$\rho_1\cup\rho_2$是A上的等价关系.

举反例如下：

设$A=\{1,2,3\}$，A上的关系

$$\rho_1=\{(1,1),(2,2),(3,3),(1,3),(3,1)\};$$

$$\rho_2=\{(1,1),(2,2),(3,3),(1,2),(2,1)\}.$$

显然ρ_1和ρ_2均是等价关系.

$$\rho_1\cup\rho_2=\{(1,1),(2,2),(3,3),(1,3),(3,1),(1,2),(2,1)\}.$$

这里$\rho_1\cup\rho_2$是自反、对称的，但不可传递.

例 2-34 设A是由4个元素组成的集合，试问在A上可以定义多少个不同的等价关系?

分析 如果直接考虑A上可以定义多少个等价关系，则计算过程比较繁琐，也容易出错.此题可利用集A上等价关系与分划1-1对应关系，转化为考虑A上有多少个不同的分划.

解 将A分划为一块：有一种方法；

将A分划为两块：2+2方式有$\frac{1}{2}C_4^2$种方法；

1+3方式有C_4^1种方法；

将A分划为三块：只能是1+1+2方式，有C_4^2种方法；

将A分划为四块：有一种方法.

因此，集A上不同等价关系的个数为

$$1+\frac{1}{2}C_4^2+C_4^1+C_4^2+1=15.$$

例 2-35 设ρ_1和ρ_2是A上的等价关系，试证明：当且仅当$\Pi_{\rho_1}^A$中的每一个等价类都包含于$\Pi_{\rho_2}^A$的某一个等价类中时，有$\rho_1\subseteq\rho_2$.

证 **充分性** 设$\Pi_{\rho_1}^A$中的每一个等价类都包含于$\Pi_{\rho_2}^A$的某一个等价类中.对任一$(a_i,a_j)\in\rho_1$，有$a_i\rho_1 a_j$，因此$a_i\in[a_i]_{\rho_1}$，

$a_j \in [a_i]_{\rho_1}$. 又由假设必有某元素 $b \in A$ 存在，使得$[a_i]_{\rho_1} \subseteq [b]_{\rho_2}$，因此有 $a_i \in [b]_{\rho_2}, a_j \in [b]_{\rho_2}$，所以$(a_i, a_j) \in \rho_2$，故有 $\rho_1 \subseteq \rho_2$.

必要性 设 $\rho_1 \subseteq \rho_2$，并设$[a_i]_{\rho_1}$是 $\Pi_{\rho_1}^A$ 中任一等价类. 对任一 $x \in [a_i]_{\rho_1}$，有 $a_i \rho_1 x$，即 $(a_i, x) \in \rho_1$，由假设 $(a_i, x) \in \rho_2$，即 $x \in [a_i]_{\rho_2}$，故有$[a_i]_{\rho_1} \subseteq [a_i]_{\rho_2}$.

下面介绍两个简单的概念.

定义 1 设 ρ 是集合 A 上的关系，若对于所有的 $a \in A$，均有 $(a,a) \notin \rho$，则称 ρ 是 A 上的反自反关系.

定义 2 集合 A 上的关系 ρ，如果它是反自反和可传递的，则称 ρ 是 A 上的拟序关系.

例如 设 $A = \{a,b,c\}$，则

$$\rho_1 = \{(a,b),(b,c)\}$$

是 A 上的反自反关系.

$$\rho_2 = \{(a,b),(b,c),(a,c)\}$$

是 A 上的拟序关系.

例 2-36 设 ρ 是集合 A 上的一个关系. 试证明

(1) 如果 ρ 是 A 上的拟序关系，则 ρ 的自反闭包 $r(\rho) = \rho \cup I_A$ 是 A 上的偏序.

(2) 如果 ρ 是一个偏序，则 $\rho - I_A$ 是一拟序.

证 (1) 对任意的 $a \in A$，有$(a,a) \in I_A$，所以$(a,a) \in \rho \cup I_A$，因此 $r(\rho)$是自反的.

对任意的 $a,b \in A$，设$(a,b) \in r(\rho)$，若 $a \neq b$，则$(a,b) \in \rho$，如果另有$(b,a) \in \rho$，则由 ρ 的可传递性，必有$(a,a) \in \rho$，这与 ρ 的反自反性相矛盾. 所以当 $a \neq b$ 时，若$(a,b) \in \rho$，必有$(b,a) \notin \rho$，因此$(b,a) \notin r(\rho)$，所以 $r(\rho)$是反对称的.

对任意的 $a,b,c \in A$，设$(a,b) \in r(\rho)$，$(b,c) \in r(\rho)$.

若$(a,b) \in I_A$，则 $a = b$，于是有$(a,c) \in r(\rho)$；

若$(b,c) \in I_A$，则 $b = c$，于是有$(a,c) \in r(\rho)$；

若$(a,b)\in\rho$且$(b,c)\in\rho$，则由ρ的可传递性，有$(a,c)\in\rho$，因此$(a,c)\in r(\rho)$，故$r(\rho)$是可传递的.

由上证得，$r(\rho)$是一偏序关系.

(2) 证明过程简单，留给读者作为练习.

例 2-37 设ρ是集合A上的偏序关系，$B\subseteq A$，试证明$\rho\cap(B\times B)$是B上的偏序关系.

证 对任意的$a\in B$，必有$(a,a)\in B\times B$，又因为$a\in A$及ρ的自反性，所以$(a,a)\in\rho$，因此$(a,a)\in\rho\cap(B\times B)$，故$\rho\cap(B\times B)$是自反的.

对任意的$a,b\in B$，若$(a,b)\in\rho\cap(B\times B)$且$(b,a)\in\rho\cap(B\times B)$，则有$(a,b)\in\rho$且$(b,a)\in\rho$，由$\rho$的反对称性，有$a=b$. 因此$\rho\cap(B\times B)$是反对称的.

对任意的$a,b,c\in B$，若$(a,b)\in\rho\cap(B\times B)$，$(b,c)\in\rho\cap(B\times B)$，则$(a,b)\in\rho$且$(b,c)\in\rho$，由$\rho$的可传递性必有$(a,c)\in\rho$；由$B\times B$的定义，$(a,c)\in B\times B$，于是$(a,c)\in\rho\cap(B\times B)$，因此$\rho\cap(B\times B)$是可传递的.

由上证得，$\rho\cap(B\times B)$是B上的偏序关系.

第三章　函　数

3.1　内容提要

1. 函数的概念

- 由集合 A 到集合 B 的函数；
- 函数的定义域和值域；
- 恒等函数；
- 复合函数；
- 逆函数.

2. 三种特殊的函数

- 由集合 A 到集合 B 的内射；
- 由集合 A 到集合 B 的满射；
- 由集合 A 到集合 B 的双射.

3. 函数的复合运算及其性质

- 函数复合运算的可结合性

  设有函数 $f:A\to B$, $g:B\to C$, $h:C\to D$，则有

$$h\cdot(g\cdot f)=(h\cdot g)\cdot f.$$

- 设 I_A 和 I_B 分别是集合 A、B 上的恒等函数，则对于任一函数 $f:A\to B$，有

$$f\cdot I_A=I_B\cdot f=f.$$

4. 复合函数的性质

- 设有函数 $f:A\to B$ 和 $g:B\to C$，那么
  (1) 如果 f 和 g 都是内射，则 $g\cdot f$ 也是内射；
  (2) 如果 f 和 g 都是满射，则 $g\cdot f$ 也是满射；
  (3) 如果 f 和 g 都是双射，则 $g\cdot f$ 也是双射.
- 设有函数 $f:A\to B$ 和 $g:B\to C$，那么
  (1) 如果 $g\cdot f$ 是内射，则 f 是内射；
  (2) 如果 $g\cdot f$ 是满射，则 g 是满射；
  (3) 如果 $g\cdot f$ 是双射，则 f 是内射，g 是满射.

5. 逆函数的有关性质

- 只有双射函数才有逆函数；
- f 的逆函数就是 f 的逆关系；
- f 的逆函数也是一个双射，且 f 和 f^{-1} 互为逆函数；
- 如果函数 $f:A\to B$ 是可逆的，则
$$f^{-1}\cdot f=I_A, f\cdot f^{-1}=I_B.$$
- 如果函数 $f:A\to B$ 和 $g:B\to C$ 均是可逆的，则
$$(g\cdot f)^{-1}=f^{-1}\cdot g^{-1}.$$

6. 集合的基数

- 集合的同基；
- 有限集与无限集；
- 可数集与不可数集；
- 集合基数的比较.

3.2 基本知识点

1. 由集合 A 到集合 B 的函数

若 f 是由集合 A 到集合 B 的一个函数，则 f 必须是由 A 到 B 的一个关系，并且对于集合 A 中的任一元素 a，在集合 B 中存在一个元素 b 且仅有这一个元素 b 使得 afb. 这样的关系 f 才称作是由 A 到 B 的函数. 若 afb，则称 b 是 a 的像，a 是 b 的像源，且记作 $f(a)=b$. 函数 f 记作 $f:A\to B$. 由此可见，由 A 到 B 的函数实际上是一个由 A 到 B 的关系，但它是满足上述条件的一种特殊的关系.

例 3-1 设 $A=\{1,2,3,4,5\}$，$B=\{6,7,8,9,10\}$分别确定下列各式中的 f 是否为由 A 到 B 的函数.

$$f=\{(1,8),(3,9),(4,10),(2,6),(5,9)\}; \tag{1}$$

$$f=\{(1,9),(3,10),(2,6),(4,9)\}; \tag{2}$$

$$f=\{(1,7),(2,6),(4,5),(1,9),(5,10),(3,9)\}. \tag{3}$$

解 (1) 式中 f 是由 A 到 B 的函数. 因为对于 A 中的每一个元素，在 B 中都有唯一一个元素与它对应.

(2) 式中 f 不是由 A 到 B 的函数. 因为 A 中的元素 5 在 B 中没有任何元素与它对应，不满足像的存在性.

(3) 式中 f 不是由 A 到 B 的函数. 因为 A 中的元素 1 在 B 中有 7 和 9 两个元素与它对应，不满足像的唯一性.

例 3-2 集合 $A=\{1,2,3\}$上的下列关系，哪些是由 A 到 A 的函数?

$$f=\{(1,3),(2,3),(3,1)\}; \tag{1}$$

$$g=\{(1,2),(3,1)\}; \tag{2}$$

$$h=\{(1,3),(2,1),(2,2)\}. \tag{3}$$

解 f 是由 A 到 A 的函数，但 g 和 h 不是由 A 到 A 的函数.

其理由读者可参照例 3-1 分析得出.

2. 恒等函数

集合 A 上的恒等关系 I_A 符合函数的定义条件,它使得 A 中每一个元素 a 均以自身为像,因此又称 I_A 为集合 A 上的恒等函数.

例 3-3 设 $A=\{1,2,3,4\}$,则

$I_A=\{(1,1),(2,2),(3,3),(4,4)\}$既称为 A 上的恒等关系,又称为 A 上的恒等函数.

若 $\rho_1=\{(1,1),(2,2),(3,3)\}$,则 ρ_1 不是 A 上的恒等函数. 因为它缺少(4,4)这一序偶.

若 $\rho_2=\{(1,1),(2,2),(3,3),(1,3),(4,4)\}$,则 ρ_2 也不是 A 上的恒等函数. 因为 $1\neq 3$,但序偶(1,3)出现在 ρ_2 中.

例 3-4 设有函数 $f:A\to A$,试证明

(1) 若 $f\subseteq I_A$,则 $f=I_A$;

(2) 若 $I_A\subseteq f$,则 $f=I_A$.

说明 这里应注意函数 f 和恒等函数 I_A 既是由集合 A 到 A 的函数,又可看作是集合 A 上的关系,而它们自身又是一个以序偶为元素的集合.

证 (1) 由题设 $f\subseteq I_A$,因此只要证明 $I_A\subseteq f$.

设 $(a,a)\in I_A$,因为 f 是由 A 到 A 的函数,所以对于元素 a,必有唯一的元素 $b\in A$,使得 $(a,b)\in f$,因为 $f\subseteq I_A$,所以 $(a,b)\in I_A$,但 I_A 是恒等函数,必有 $b=a$,因此 $(a,a)\in f$. 由 a 的任意性,有 $I_A\subseteq f$,于是 $f=I_A$.

(2) 由题设 $I_A\subseteq f$,因此只要证明 $f\subseteq I_A$.

设 $(a,b)\in f$,则 $a\in A$,因为 I_A 是恒等函数,所以 $(a,a)\in I_A$,由 $I_A\subseteq f$ 可知 $(a,a)\in f$,由 $(a,b)\in f$ 和 $(a,a)\in f$ 且 f 是函数,必有 $a=b$,即 $(a,b)=(a,a)$,所以 $(a,b)\in I_A$,即 $f\subseteq I_A$. 于是 $f=I_A$.

3. 内射、满射和双射

设 f 是一由 A 到 B 的函数，若对于 A 中任意两个元素 a_i 和 a_j，当 $a_i \neq a_j$ 时，一定有 $f(a_i) \neq f(a_j)$，则称 f 是由 A 到 B 的内射；若对于 B 中任一元素 b，一定存在有 $a \in A$，使得 $f(a)=b$，则称 f 是由 A 到 B 的满射；若 f 既是内射又是满射，则称 f 是由 A 到 B 的双射.

例 3-5 在下列函数中，确定哪些是内射、哪些是满射、哪些是双射.

(1) $f_1: R \to R, f_1(r)=r^2+2r-15$；

(2) $f_2: N^2 \to N, f_2(n_1,n_2)=n_1^{n_2}$；

(3) $f_3: (2^U)^2 \to (2^U)^2, f_3(s_1,s_2)=(s_1 \cup s_2, s_1 \cap s_2)$；

(4) $f_4: Z_7 \to Z_7, f_4(x)=\text{res}_7(3x)$.

其中 R 表示实数集，N 表示正整数集，U 表示全集合，$Z_7=\{0,1,2,3,4,5,6\}$.

解 (1) 因为 $f_1(-5)=f_1(3)=0$，所以 f_1 不是内射.

$f_1(r)=(r^2+2r+1)-16=(r+1)^2-16$. 显然对于任意的 $r \in R$，均有 $(r+1)^2 \geqslant 0$，所以对于任意的 $r \in R$，$f_1(r) \geqslant -16$. 这就是说，当 $y<-16$ 时，y 在 R 中无像源，因此 f_1 不是满射. 由此可知 f_1 也不是双射.

(2) 因为 $f_2(4,1)=f_2(2,2)=4^1=2^2=4$，所以 f_2 不是内射.

对于任意的 $n \in N$，有 $f_2(n,1)=n1=n$. 即对于任意的 $n \in N$，n 有像源 $(n,1)$，所以 f_2 是满射. 但 f_2 不是双射.

(3) 对任意 $s_1 \in 2^U$ 和 $s_2 \in 2^U$，若 $s_1 \neq s_2$，则 $(s_1,s_2) \neq (s_2,s_1)$. 而

$$f_3(s_1,s_2) = (s_1 \cup s_2, s_1 \cap s_2);$$

$$f_3(s_2,s_1) = (s_2 \cup s_1, s_2 \cap s_1).$$

由集合并运算和交运算的可交换性，有

$$f_3(s_1,s_2) = f_3(s_2,s_1).$$

因此 f_3 不是内射.

又$(\varnothing,U)\in(2^{v})^2$，但不存在$s_1\in 2^{v}$和$s_2\in 2^{v}$，使得$s_1\cup s_2=\varnothing$，而$s_1\cap s_2=U$，即$(\varnothing,U)$在$(2^{v})^2$中没有像源，所以$f_3$也不是满射. 因此$f_3$不是双射.

(4) $\mathrm{res}_7(3x)$表示$3x$被7除后的非负余数，于是按照函数f_4的定义

$$f_4(0)=\mathrm{res}_7(0)=0,\quad f_4(4)=\mathrm{res}_7(12)=5,$$
$$f_4(1)=\mathrm{res}_7(3)=3,\quad f_4(5)=\mathrm{res}_7(15)=1,$$
$$f_4(2)=\mathrm{res}_7(6)=6,\quad f_4(6)=\mathrm{res}_7(18)=4.$$
$$f_4(3)=\mathrm{res}_7(9)=2,$$

显然f_4既是内射又是满射，因此f_4是一个双射.

4. 复合函数

若有函数$f:A\to B$和$g:B\to C$，那么我们可以根据f和g定义一个由A到C的新函数$g\cdot f:A\to C$. 定义的方法是对于集合A中的每一个元素a，若$f(a)=b$，而$g(b)=c$，则定义$g\cdot f(a)=c$. 也就是说，若元素a在函数f作用下的像是b，而b在函数g作用下的像是c，则定义a在复合函数$g\cdot f$作用下的像为c，即$g\cdot f(a)=g(f(a))=g(b)=c$.

由于f和g均是函数，因此$f(a)$的存在和唯一以及$g(b)$的存在和唯一保证了$g\cdot f(a)$的存在和唯一. 因而也就保证了这样定义的$g\cdot f$必是一由A到C的函数. 我们常将$g\cdot f$简记作gf.

例 3-6 设有函数$f:R\to R$，$g:R\to R$和$h:R\to R$（R表示实数集），且有$f(x)=x+5$，$g(x)=3x+1$，$h(x)=\frac{x}{2}$. 试求复合函数$g\cdot f$、$f\cdot g$和$f\cdot h$.

解 由复合函数的定义，所求的复合函数均是由R到R的函数.

$$g\cdot f(x)=g(f(x))=g(x+5)=3(x+5)+1=3x+16;$$
$$f\cdot g(x)=f(g(x))=f(3x+1)=3x+1+5=3x+6;$$

$$f\cdot h(x)=f(h(x))=f(\frac{x}{2})=\frac{x}{2}+5.$$

例 3-7 设有函数 $f:R\to R$ 和 $g:R\to R$(R 表示实数集)

$$f(x)=\begin{cases}x^2 & x\geqslant 3;\\ -2 & x<3,\end{cases}\quad g(x)=x+2,$$

试求复合函数 $f\cdot g$ 和 $g\cdot f$.

解 复合函数 $f\cdot g$ 和 $g\cdot f$ 均是由 R 到 R 的函数.

$$f\cdot g(x)=f(g(x))=f(x+2)=\begin{cases}(x+2)^2, & x+2\geqslant 3;\\ -2, & x+2<3,\end{cases}$$

即

$$f\cdot g(x)=\begin{cases}(x+2)^2, & x\geqslant 1;\\ -2, & x<1,\end{cases}$$

$$g\cdot f(x)=g(f(x))=\begin{cases}g(x^2), & x\geqslant 3;\\ g(-2), & x<3,\end{cases}$$

$$=\begin{cases}x^2+2, & x\geqslant 3;\\ 0, & x<3.\end{cases}$$

例 3-8 设有函数 $f:R\to R$ 和 $g:R\to R$,这里 $f(x)=x^2-2$,$g(x)=x+4$,试求出复合函数 $f\cdot g$ 和 $g\cdot f$,并说明这些函数是否内射、满射或双射.

解 $f\cdot g(x)=f(x+4)=(x+4)^2-2$;

$g\cdot f(x)=g(x^2-2)=x^2-2+4=x^2+2$.

(1) 因为 $f(2)=f(-2)$,所以 f 不是内射. 又因为对于任意的 $x\in R$,$f(x)\geqslant -2$,所以 f 也不是满射,故 f 不是双射.

(2) 因为当 $x_1\neq x_2$ 时,$x_1+4\neq x_2+4$,所以 g 是内射. 又对于任一 $y\in R$,$g(y-4)=y$. 即实数集 R 中任一实数 y 都有像源 $y-4$,所以 g 是满射,因此 g 是双射.

(3) 因为对于任意 $x\in R$,$f\cdot g(x)=(x+4)^2-2\geqslant -2$,这说明当 $y<-2$ 时 y 在 R 中没有像源,因此 $f\cdot g$ 不是满射. 又因为 $fg(0)=fg(-8)$,所以 $f\cdot g$ 不是内射. 因此 $f\cdot g$ 不是双射.

(4) 因为对任意 $x\in R$,有 $x^2+2\geqslant 2$,所以 $g\cdot f$ 不是满射. 又

因为对于任意 $x\in R$，$g\cdot f(x)=g\cdot f(-x)$，所以 $g\cdot f$ 也不是内射. 因此 $g\cdot f$ 不是双射.

例 3-9 设 $A=\{1,2,3,4\}$，定义一个函数 $f:A\to A$，使得 f 是双射但 $f\neq I_A$，求 f^2、f^3. 能否找到一个双射 $g:A\to A$，使 $g\neq I_A$ 但 $g^2=I_A$.

解 定义函数 $f:A\to A$. 使得 $f(1)=2,f(2)=3,f(3)=4,f(4)=1$. 显然 f 是双射且 $f\neq I_A$.

函数 $f^2:A\to A,f^2(1)=3,f^2(2)=4,f^2(3)=1,f^2(4)=2$;

函数 $f^3:A\to A,f^3(1)=f^2(f(1))=f^2(2)=4$.

类似地 $f^3(2)=1,f^3(3)=2,f^3(4)=3$.

可定义函数 $g:A\to A$ 使得 $g(1)=2,g(2)=1,g(3)=4,g(4)=3$. 显然 $g\neq I_A$，但 $g^2=I_A$.

5. 复合函数的性质

在内容提要中，我们介绍了复合函数的两条性质. 即由函数 $f:A\to B$ 和函数 $g:B\to C$ 的性质可以决定复合函数 $g\cdot f:A\to C$ 的性质；反过来，由 $g\cdot f$ 的性质可部分地决定 f 和 g 的性质.

例 3-10 设有函数 $f:A\to B,g:B\to A$ 且 $g\cdot f$ 是 A 上的恒等函数，试证明 f 是内射，g 是满射.

证 因为 $g\cdot f:A\to A$ 是恒等函数，所以 $g\cdot f$ 是双射. 由复合函数的性质，f 必是内射而 g 必是满射.

要注意的是，当复合函数 $g\cdot f:A\to C$ 是内射时，虽然可推出 f 一定是内射，但 g 可以不是内射. 图 3-1 给出了这种情形的一个例子. 但如果我们限定 f 是一个满射时，则又是不同的结果了.

例 3-11 设有函数 $f:A\to B$ 和 $g:B\to C$，且 $g\cdot f$ 是内射，f 是满射. 试证明 g 是内射. 举一个例子说明，若 f 不是满射，则 g 不一定是内射.

分析 根据内射的定义，在 B 中任取两个元素 b_1 和 b_2，假设 $b_1\neq b_2$，证明 $g(b_1)\neq g(b_2)$ 即可. 在证明的过程中需要用到 f 是满

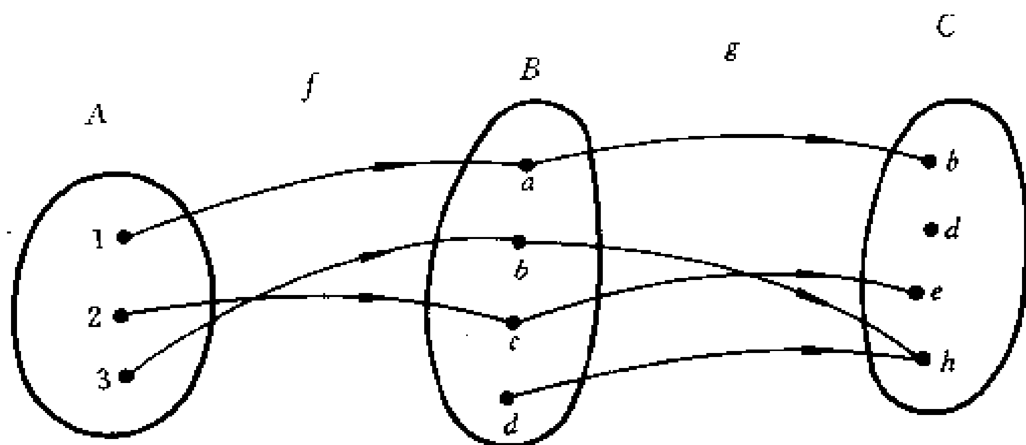


图 3-1

射和 $g \cdot f$ 是内射的条件，因此还需与 A 中的元素发生关系.

证 任取 $b_1, b_2 \in B$，并设 $b_1 \neq b_2$，因为 f 是满射，所以必有 $a_1, a_2 \in A$，使得 $f(a_1)=b_1, f(a_2)=b_2$，由于 $b_1 \neq b_2$，根据函数的定义，必有 $a_1 \neq a_2$. 又因为 g 是由 B 到 C 的函数，所以有 $c_1, c_2 \in C$，使得 $g(b_1)=c_1, g(b_2)=c_2$. 于是根据复合函数的定义，

$$g \cdot f(a_1) = g(b_1) = c_1,\ g \cdot f(a_2) = g(b_2) = c_2.$$

因为 $g \cdot f$ 是内射，所以由 $a_1 \neq a_2$ 可知 $c_1 \neq c_2$. 此即 $g(b_1) \neq g(b_2)$，故 g 是内射.

图 3-1 中的例子可说明当 f 不是满射时，g 不一定是内射.

类似地，当复合函数 $g \cdot f: A \to C$ 是满射，虽然可推出 g 是满射，但 f 可以不是满射. 但是，如果我们限定 g 是内射时，则又是不同的结果了.

例 3-12 设有函数 $f: A \to B$ 和 $g: B \to C$，且 $g \cdot f$ 是满射，g 是内射. 试证明 f 是满射. 举一个例子说明，若 g 不是内射，则 f 不一定是满射.

分析 根据满射的定义，在 B 中任取一元素 $b \in B$，证明在 A 中必存在一元素 $a \in A$ 使得 $f(a)=b$ 即可. 在证明过程中需要用到 $g \cdot f$ 是满射和 g 是内射的条件，因此还需与 C 中的元素发生关系.

证 对任一 $b \in B$，因为 g 是由 B 到 C 的函数，所以必有

$c \in C$，使 $g(b)=c$. 又因为 $g \cdot f$ 是满射，所以又必有 $a \in A$，使 $g \cdot f(a)=c$，$g \cdot f(a)=g(f(a))=c$，令 $f(a)=b'$，则有 $g(b')=c$. 于是有 $g(b)=g(b')=c$，但 g 是内射，必有 $b=b'$. 此即 $f(a)=b$，因此 f 是一满射.

图 3-2 中复合函数 $g \cdot f$ 是满射，g 不是内射，f 不是满射.

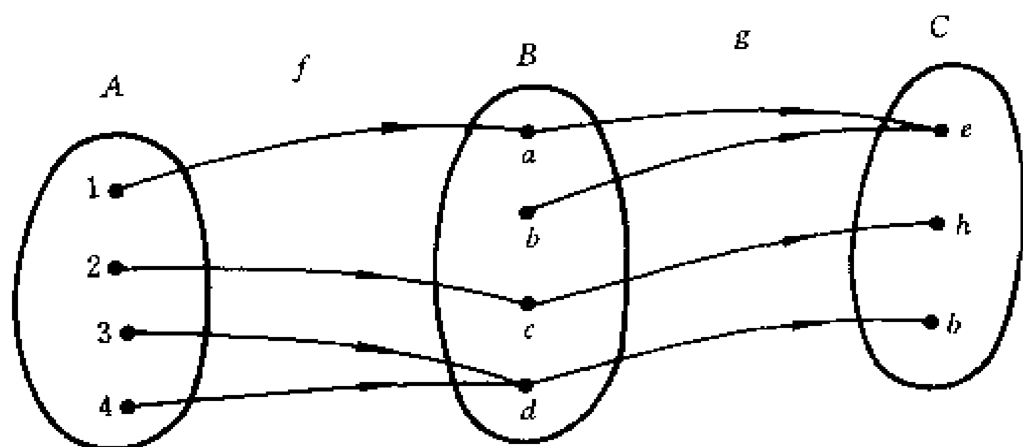


图 3-2

6. 函数复合运算的性质

由函数 $f:A \to B$ 和 $g:B \to C$ 求复合函数 $g \cdot f:A \to C$ 的过程称为函数的复合运算. 在内容提要中，我们介绍了函数的复合运算满足结合律. 事实上，函数复合运算的可结合性可以推广到任意 n 个函数. 若有函数 $f_1:A_1 \to A_2, f_2:A_2 \to A_3, \cdots, f_n:A_n \to A_{n+1}$，则可以对表达式 $f_n \cdot f_{n-1} \cdot \cdots \cdot f_2 \cdot f_1$ 任意加括号，所得到的复合函数都是相同的. 因此我们常使用不加括号的表达式 $f_n \cdot f_{n-1} \cdot \cdots \cdot f_2 \cdot f_1$，它唯一地表示一个由 A_1 到 A_{n+1} 的函数.

例 3-13 设有函数 $f:A \to A$，若存在一正整数 n 使得 $f^n=I_A$，试问你可否判断 f 是否内射、满射或双射？

解 若 $n=1$，则 $f=I_A$. 因为恒等函数 I_A 是双射，所以 f 是双射.

若 $n>1$，则由复合函数的可结合性，得

$$f^n = f^{n-1} \cdot f = f \cdot f^{n-1} = I_A.$$

由 $f^{n-1} \cdot f = I_A$ 和 I_A 是内射，可知 f 是内射.

由 $f \cdot f^{n-1} = I_A$ 和 I_A 是满射，可知 f 是满射，故可判断 f 是一个双射.

7. 函数的定义域和值域

设 f 是一由集合 A 到 B 的函数，因为对于 A 中每一个元素，在集合 B 中均有元素与之对应，所以 f 的定义域 $D_f = A$. 但对于任一函数 f 来说，B 中的每一个元素在 A 中不一定有像源，因此 f 的值域 $R_f \subseteq B$. 只有当 f 是满射时，才有 $R_f = B$.

我们常用符号 $f(A)$ 表示函数 f 的值域，即

$$f(A) = \{b \mid b \in B, \text{存在}\ a \in A, \text{使得}\ f(a) = b\}.$$

若 $S \subseteq A$，则 S 中所有元素的像的集合也通常记作 $f(S)$，即

$$f(S) = \{b \mid b \in B, \text{存在}\ a \in S, \text{使得}\ f(a) = b\}.$$

例 3-14 设有函数 $f: A \to B, S \subseteq A$，等式

$$f(A) - f(S) = f(A - S)$$

成立吗？为什么？

解 根据前面的定义，式中的 $f(A)$、$f(S)$、$f(A-S)$ 均是 B 的子集，因此 $f(A) - f(S)$ 也是 B 的子集.

下面证明 $f(A) - f(S) \subseteq f(A-S)$.

设 $b \in f(A) - f(S)$，则 $b \in f(A)$ 且 $b \notin f(S)$，所以必存在 $a \in A$ 使 $f(a) = b$. 由于 $b \notin f(S)$，所以 $a \notin S$，于是 $a \in A - S$，因此 $b \in f(A-S)$，故 $f(A) - f(S) \subseteq f(A-S)$.

但是，对于任意的函数 $f: A \to B$，$f(A-S) \subseteq f(A) - f(S)$ 不成立. 分析如下：

若设 $b \in f(A-S)$，则可推出必有 $a \in A - S$，使得 $f(a) = b$. 但根据函数的定义，此时并不排斥同时可能有元素 $a' \in S$，也使得 $f(a') = b$，这样一来就有可能 $b \in f(S)$，而导致 $b \notin f(A) - f(S)$.

举反例如下：

设 $A = \{a_1, a_2, a_3, a_4\}$，$S = \{a_2, a_3\}$，则 $A - S = \{a_1, a_4\}$，函数

$f: A \to B$ 的定义如图 3-3 所示.

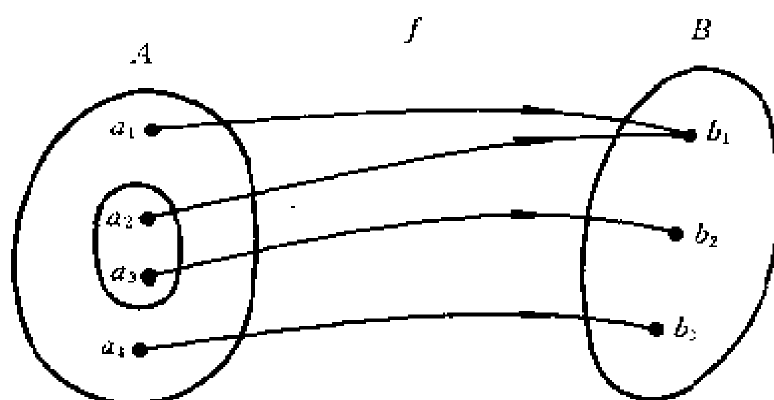


图 3-3

显然
$$f(A)=\{b_1,b_2,b_3\};$$
$$f(S)=\{b_1,b_2\};$$
$$f(A-S)=\{b_1,b_3\};$$
$$f(A)-f(S)=\{b_3\};$$
$$f(A-S)\not\subseteq f(A)-f(S).$$

由上可知,等式 $f(A)-f(S)=f(A-S)$ 不成立.

例 3-15 设 f 和 g 是函数,且有 $f\subseteq g$ 和 $D_g\subseteq D_f$,试证明 $f=g$.

分析 题目只告诉我们 f 和 g 是函数,并没有告诉我们它们是由哪一个集合到哪一个集合的函数. 这并不影响我们证明 $f=g$.

一个函数实际上是一个关系,因此函数是由序偶组成的集合. 若能证明 f 和 g 是由相同的序偶所组成,则意味着 f 和 g 是相同的函数,即 $f=g$. 由题设已知 $f\subseteq g$,因此只要证明 $g\subseteq f$ 即可.

证 设 $(a,b)\in g$,则 $g(a)=b$,所以 $a\in D_g$. 因为 $D_g\subseteq D_f$,所以 $a\in D_f$,于是必有 b' 使 $f(a)=b'$,即 $(a,b')\in f$. 由题设 $f\subseteq g$,所以 $(a,b')\in g$,由于 g 是函数,必有 $b=b'$,于是 $(a,b)\in f$,故 $g\subseteq f$. 又由题设 $f\subseteq g$,因此 $f=g$.

8. 逆函数

设有函数 $f:A\to B$，若 f 不是内射，则 f 的逆关系 $\tilde{f}$ 必使得 B 中至少有一个元素 b，与 A 中多个不同的元素相对应，因此 $\tilde{f}$ 不能成为函数.

若 f 不是满射，则 f 的逆关系 $\tilde{f}$ 必使得 B 中至少有一个元素 b，在 A 中没有元素与其对应. 因此 $\tilde{f}$ 也不能成为函数.

若 f 是一个双射；则因为 f 是满射，它必使得 B 中每一元素 b 在 A 中有像源. 又因为 f 是内射，b 的像源必是唯一的，因此逆关系 $\tilde{f}$ 是一由 B 到 A 的函数. 我们称它为 f 的逆函数. 记作 f^{-1}. 由上可知，只有当 f 是双射时，f 才有逆函数. 而且容易证明 f^{-1} 也是一个双射.

例 3-16 下列四个函数是否存在逆函数？若有，则求出其逆函数（R 表示实数集）.

(1) $f_1:R\to R$，　$f_1(x)=x^2$；

(2) $f_2:R\to R$，　$f_2(x)=2^x$；

(3) $f_3:R\to R$，　$f_3(x)=x^2-2x-3$；

(4) $f_4:R\to R$，　$f_4(x)=x^3$.

解 要判断上述函数是否存在逆函数，实际上是要判断上述函数是否为双射.

(1) 因为 $f_1(2)=f_1(-2)=4$，且当 y 为负数时，没有像源，所以 f_1 既不是内射，又不是满射. 因此 f_1 没有逆函数.

(2) 对于任意的 $x\in R$，有 $f_2(x)>0$，因此 f_2 不是满射，所以 f_2 没有逆函数.

(3) $f_3(x)=x^2-2x-3=(x+1)(x-3)=(x-1)^2-4$，显然 $f_3(-1)=f_3(3)=0$，因此 f_3 不是内射. 又对于任意的 $x\in R$，$f_3(x)\geqslant -4$，因此 f_3 也不是满射，故 f_3 没有逆函数.

(4) f_4 既是内射，又是满射，所以 f_4 是双射. 它有逆函数

$f_4^{-1}: R \to R, f_4^{-1}(y) = \sqrt[3]{y}$.

若作出各函数的图象，亦可直观地得出上述结论.

利用逆函数的概念，我们可以用更简单的方法来证明例 3-11 和例 3-12.

例 3-11 的证法二如下：

证 因为 $g \cdot f$ 是内射，所以 f 是内射. 又因为 f 是满射，所以 f 是双射. 于是有逆函数 $f^{-1}: B \to A$ 且 f^{-1} 也是双射. 根据函数复合运算的可结合性

$$g \cdot f \cdot f^{-1} = (g \cdot f) \cdot f^{-1} = g \cdot (f \cdot f^{-1}) = g \cdot I_B = g.$$

因为 $g \cdot f$ 是内射，f^{-1} 也是内射，所以 g 是内射.

仿照例 3-11，可类似地给出例 3-12 的证法二. 这留给读者作为练习.

9. 数学归纳法

数学归纳法是读者早已熟悉的一种证明方法. 实际上，数学归纳法除了可以用来证明与自然数有关的命题外，还可以利用数学归纳法的原理来定义函数和集合.

例 3-17 阿克曼(Ackerman)函数 $A: Z^2 \to Z$ 归纳地定义如下：

$$A(0,n) = n + 1 \quad (n \geqslant 0);$$

$$A(m,0) = A(m-1,1) \quad (m > 0);$$

$$A(m,n) = A(m-1, A(m,n-1)) \quad (m > 0, n > 0),$$

试计算 $A(2,3)$.

解 为计算 $A(2,3)$，我们采用数学归纳法来证明 $A(2,n)$ 的一般计算公式.

当 $m=0$ 时，$A(0,n)=n+1 \quad (n \geqslant 0)$；

当 $m=1$ 时，若 $n=0$，则 $A(1,0)=A(0,1)=2=0+2$；

若 $n=1$，则 $A(1,1)=A(0,A(1,0))=A(1,0)+1$

$$=3=1+2,$$

假设 $A(1,n-1)=(n-1)+2 \quad (n\geqslant 1)$，则

$$\begin{aligned} A(1,n) &= A(0,A(1,n-1)) \\ &= A(1,n-1)+1 \\ &= (n-1)+2+1 \\ &= n+2, \end{aligned}$$

因此，当 $m=1$ 时，$A(1,n)=n+2 \quad (n\geqslant 0)$，

当 $m=2$ 时，若 $n=0$，则 $A(2,0)=A(1,1)=3=2\cdot 0+3$；

若 $n=1$，则 $A(2,1)=A(1,A(2,0))=A(2,0)+2$

$$=5=2\cdot 1+3.$$

假设 $A(2,n-1)=2\cdot(n-1)+3 \quad (n\geqslant 1)$，

则
$$\begin{aligned} A(2,n) &= A(1,A(2,n-1))=A(2,n-1)+2 \\ &= 2\cdot(n-1)+3+2=2\cdot n+3. \end{aligned}$$

因此，当 $m=2$ 时，$A(2,n)=2\cdot n+3 \quad (n\geqslant 0)$.

由此可知，$A(2,3)=2\cdot 3+3=9$.

10. 集合的基数

前面曾将集合的基数定义为集合中不同元素的个数，这种定义方法对于无限集来说，显得过于简单，因此，我们引进集合同基的概念. 对于集合 A、B，如果存在一个双射函数 $f:A\to B$，则称集合 A 与 B 有相同的基数. 或者说 A 与 B 同基（或 A 与 B 等势），常记作 $A\sim B$.

若集合 A 与 B 同基，即若有双射函数 $f:A\to B$，则 f 的逆函数 $f^{-1}:B\to A$ 也是一个双射函数，因此 B 也与 A 同基. 因此集合的同基关系是对称的. 容易证明它也是自反和可传递的. 因此同基关系是一个等价关系.

例 3-18 证明 $[0,1)$ 与 $(0,1)$ 同基. $[0,1)$ 与 $[0,1]$ 同基.

证 设 $A=\{0,\frac{1}{2},\frac{1}{3},\cdots,\frac{1}{n},\cdots\}$，定义函数 $f:[0,1)\to(0,1)$ 如下

$$f(x)=\begin{cases}\dfrac{1}{2}, & x=0;\\ \dfrac{1}{n+1}, & x=\dfrac{1}{n} \text{ 且 } n\geqslant 2;\\ x, & x\in[0,1)-A.\end{cases}$$

显然 f 是一双射函数,所以 $[0,1)$ 与 $(0,1)$ 同基.

定义函数 $g:[0,1)\to[0,1]$ 如下:

$$g(x)=\begin{cases}0, & x=0;\\ \dfrac{1}{n-1}, & x=\dfrac{1}{n} \text{ 且 } n\geqslant 2;\\ x, & x\in[0,1)-A.\end{cases}$$

显然 g 也是一双射函数,所以 $[0,1)$ 与 $[0,1]$ 同基.

由于同基关系具有对称性和可传递性,因此 $(0,1)$ 与 $[0,1]$ 同基.

一个无限集如果它与正整数集 N 同基,则称它为可数集,否则称它为不可数集. 如整数集 I、有理数集 Q、所有奇数的集合和所有偶数的集合等均是可数集,它们具有相同的基数,记作 $\aleph_0$. [1]中也列举了许多的不可数集,如 $(0,1)$,$[0,1]$,实数集 R 等均是不可数集,且它们相互同基,因此它们具有相同的基数,称作连续基数,记作 $\aleph_0$. 对此[1]中均有详细的证明和叙述,这里不再赘述.

在定义了集合同基的概念后,可以进一步定义集合之间基数大小的比较. 下面我们仍用符号 $\#A$ 来表示集合 A 的基数. 对于任意两个集合 A、B,若存在双射 $f:A\to B$,则 $\#A=\#B$;若 A 与 B 之间不存在双射,存在内射 $f:A\to B$,则 $\#A<\#B$;若只知由 A 到 B 存在内射,不知由 A 到 B 是否存在双射,则可记 $\#A\leqslant\#B$.

定理 设 A,B 是两个集合,若有 $A_1\subseteq A$ 和 $B_1\subseteq B$ 使得 $A\sim B_1$,$B\sim A_1$,则 $A\sim B$.

例 3-19 利用上述定理证明 $[0,1]\sim(0,1)$.

证 显然 $(0,1)\subseteq[0,1]$. 定义函数 $f:(0,1)\to[0,1]$ 使得

$$f(x) = x.$$

这是由(0,1)到(0,1)的一个双射,所以$(0,1)\sim(0,1)$.

又$[\frac{1}{4},\frac{3}{4}]\subseteq(0,1)$,定义函数$g:[0,1]\to[\frac{1}{4},\frac{3}{4}]$使得

$$f(x) = \frac{x}{2} + \frac{1}{4},$$

这是由[0,1]到$[\frac{1}{4},\frac{3}{4}]$的一个双射,所以$[0,1]\sim[\frac{1}{4},\frac{3}{4}]$.

由上述定理可得,$[0,1]\sim(0,1)$.

3.3 问答与论证

例 3-20 设$A=\{a,b,c\}$,$B=\{p,q\}$,试问有多少个由A到B的函数?有多少个由A到B的满射?

解 记由A到B的所有函数的集合为B^A,即

$$B^A = \{f \mid f:A \to B\}.$$

由$\#(B^A)=\#B^{\#A}$可知,本例中由A到B的函数的个数$\#B^{\#A}=2^3=8$(个).

由$\#A>\#B$可知,由A到B不存在双射,也不存在内射,但存在满射是可能的.有多少个满射呢?可分别用以下两种方法计算.

方法一 计算非满射的函数个数.

函数$f:A\to B$若不是满射,则只有两种情形,或者$f(a)=f(b)=f(c)=p$,或者$f(a)=f(b)=f(c)=q$,因此非满射的函数仅2个,故由A到B的满射为6个.

方法二 直接计算满射函数的个数.

函数$f:A\to B$若为满射,则必是A中两个元素对应于B中同一个元素,而另一个元素对应于B中剩下的那个元素.

若是两个元素对应于p,则函数个数为C_3^2.

若是两个元素对应于q,则函数个数也为C_3^2.因此满射函数个

数为 $2 \cdot C_3^2 = 2 \cdot 3 = 6$(个).

例 3-21 试证明若 $A \subseteq B$,则 $A^C \subseteq B^C$.

分析 A^C 和 B^C 正如例 3-20 中所解释的,它们分别表示由集合 C 到集合 A 的所有函数的集合和由集合 C 到集合 B 的所有函数的集合.

证 设 $f \in A^C$,则 f 是一由 C 到 A 的函数,于是对于任意 $c \in C$,必有唯一的 $a \in A$,使得 $f(c)=a$,因为 $A \subseteq B$,所以 $a \in B$,因此,对于任意 $c \in C$,必有唯一的 $a \in B$,使得 $f(c)=a$. 根据函数的定义,f 也是一由 C 到 B 的函数. 即 $f \in B^C$,故 $A^C = B^C$.

例 3-22 设有函数 $f: A \cup B \to C$,试证明

$$f(A) \cup f(B) = f(A \cup B).$$

证 设 $c \in f(A) \cup f(B)$,则 $c \in f(A)$ 或 $c \in f(B)$. 若 $c \in f(A)$,则存在 $a \in A$ 使得 $f(a)=c$,因此有 $a \in A \cup B$,所以 $c \in f(A \cup B)$. 若 $c \in f(B)$,类似地,亦有 $c \in f(A \cup B)$,故 $f(A) \cup f(B) \subseteq f(A \cup B)$.

反之,若 $c \in f(A \cup B)$,则存在 $b \in A \cup B$,使得 $f(b)=c$. 由并集的定义 $b \in A$ 或 $b \in B$,因此 $c \in f(A)$ 或 $c \in f(B)$,于是 $c \in f(A) \cup f(B)$,故 $f(A \cup B) \subseteq f(A) \cup f(B)$.

由上证得 $f(A) \cup f(B) = f(A \cup B)$.

例 3-23 设有函数 $f: A \cup B \to C$,试问 $f(A) \cap f(B) = f(A \cap B)$成立吗? 为什么?

解 $f(A \cap B) \subseteq f(A) \cap f(B)$是成立的. 证明如下:

设 $c \in f(A \cap B)$,则存在 $a \in A \cap B$ 使得 $f(a)=c$. 因为 $a \in A$ 且 $a \in B$,所以 $c \in f(A)$且 $c \in f(B)$,因此 $c \in f(A) \cap f(B)$,故 $f(A \cap B) \subseteq f(A) \cap f(B)$.

但 $f(A) \cap f(B) \subseteq f(A \cap B)$不成立.

为了说明这一论断,我们设 $c \in f(A) \cap f(B)$,于是由交集的定义有 $c \in f(A)$且 $c \in f(B)$.

由 $c \in f(A)$可知,存在某个元素 $a \in A$,使得 $f(a)=c$;

由 $c\in f(B)$ 可知，存在某个元素 $b\in B$，使得 $f(b)=c$.

但我们无法推出 $A\cap B$ 中一定有元素 d 使得 $f(d)=c$. 反例如下：

设 $A\cup B=\{a,b,e,d\}$，其中 $A=\{a,e,d\}$，$B=\{b,e\}$，$C=\{c_1,c_2,c_3\}$，函数 $f:A\cup B\to c$ 定义为 $f(a)=f(b)=c_1$，$f(e)=c_2$，$f(d)=c_3$，于是

$$A\cap B=\{e\},f(A\cap B)=\{c_2\},$$
$$f(A)=\{c_1,c_2,c_3\},f(B)=\{c_1,c_2\},$$
$$f(A)\cap f(B)=\{c_1,c_2\}.$$

这里元素 $c_1\in f(A)\cap f(B)$，但 $c_1\notin f(A\cap B)$.

例 3-24 设有函数 $f:A\to B$，$B'\subseteq B$，定义

$$N(B')=\{a\mid a\in A \text{ 且 } f(a)\in B'\}.$$

(1) 试证明 $f(N(B'))\subseteq B'$；

(2) 在什么情形下有 $f(N(B'))=B'$？

分析 要能正确解答此题，首先必须清楚各个符号的含义.

$N(B')$ 是 A 的子集，它是由集合 B' 中所有元素的像源组成的集合.

$f(N(B'))$ 是 B 的子集，它是由 $N(B')$ 中所有元素的像组成的集合.

证 (1) 设 $b\in f(N(B'))$，则存在 $a\in N(B')$，使得 $f(a)=b$. 由 $N(B')$ 的定义 $f(a)\in B'$，即 $b\in B'$，故 $f(N(B'))\subseteq B'$.

解 (2) 当 $B'\subseteq f(A)$ 时，有 $f(N(B'))=B$.

在证明这一结论之前，我们先看一例. 如图 3-4 所示.

f 是一由 A 到 B 的函数，设 $B'=\{2,3,4\}$，根据定义 $N(B')=\{b,c,d\}$，但由于 B' 中的元素 4 在 A 中无像源，因此 $N(B')$ 经 f 映射后，

$$f(N(B'))=\{2,3\}\neq B',$$

由此可知，要使 $f(N(B'))=B'$，必须 B' 中每一元素均有像源.

下面给出一般的证明：

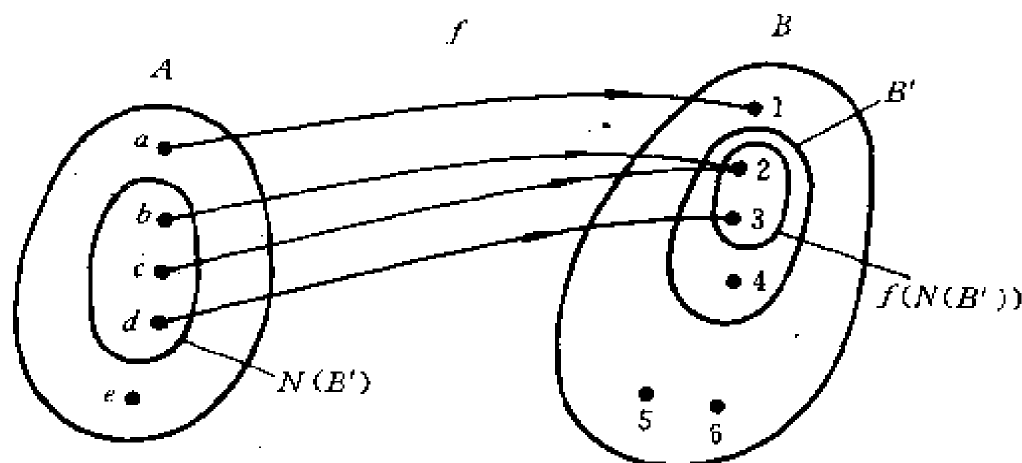


图 3-4

由(1)可知 $f(N(B'))\subseteq B'$，我们只要证明 $B'\subseteq f(N(B'))$ 即可.

设 $b\in B'$，因为 $B'\subseteq f(A)$，所以必有 $a\in A$，使得 $f(a)=b$. 由 $N(B')$ 的定义，$a\in N(B')$，因此 $f(a)\in f(N(B'))$，即 $b\in f(N(B'))$，故 $B'\subseteq f(N(B'))$.

例 3-25 设有函数 $f:A\to A$，$g:A\to A$ 和 $h:A\to A$，使得复合函数 $h\cdot f=h\cdot g$. 试证明若 h 是一内射，则 $f=g$.

证 (反证法)假设 $f\neq g$，则必存在元素 $a\in A$，使得 $f(a)\neq g(a)$，因为 h 是内射，所以 $h(f(a))\neq h(g(a))$，即 $h\cdot f(a)\neq h\cdot g(a)$. 这与题设 $h\cdot f=h\cdot g$ 相矛盾. 故 $f=g$.

例 3-26 设有函数 $f:A\to B$，定义函数 $g:B\to 2^A$，使得

$$g(b)=\{a\mid a\in A, f(a)=b\},$$

试证明如果 f 是满射，则 g 是内射. 其逆成立吗?

证 **证法一** 设 $b_1,b_2\in B$，$b_1\neq b_2$，因为 f 是满射，所以必有 $a\in A$，使得 $f(a)=b_1$，由函数的定义，$f(a)\neq b_2$. 因此 $a\in g(b_1)$，$a\notin g(b_2)$，于是 $g(b_1)\neq g(b_2)$，故 g 是一内射.

证法二(反证法)假设 g 不是内射，则必存在 $b_1,b_2\in B$，$b_1\neq b_2$，但 $g(b_1)=g(b_2)=A_i$，因为 f 是满射，所以 $A_i\neq\varnothing$，因此 A_i 中至少

存在一个元素 a，满足 $f(a)=b_1$，$f(a)=b_2$，然而 $b_1\neq b_2$，这与 f 是一个函数相矛盾，故 g 是一内射.

其逆不成立. 因为当 g 是内射时，可能有一个元素 b 使 $g(b)=\varnothing$，这意味着元素 $b\in B$ 在 A 中没有像源. 因此 f 不是满射.

例如　设 $A=\{a_1,a_2,a_3\}$，$B=\{b_1,b_2,b_3\}$，函数 f 和 g 的定义如图 3-5 所示. 此时 g 是内射，但 f 不是满射.

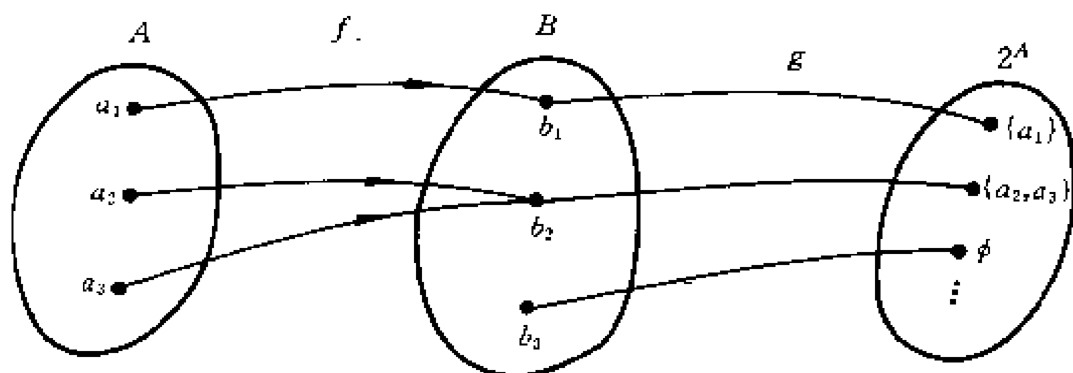


图 3-5

例 3-27　设有集合 A、B，其中 $A=\{a_1,a_2,\cdots,a_n\}$，又设 $F=\{f|f:A\to B\}$，函数 $g:F\to B^n$ 定义为对于每一 $f\in F$，$g(f)=(f(a_1),f(a_2),\cdots,f(a_n))$，试证明 g 是一个双射.

分析　注意记号 B^n 表示笛卡尔积

$$\underbrace{B\times B\times\cdots\times B}_{n\text{个}}=\{(b_{i_1},b_{i_2},\cdots,b_{i_n})|b_{i_j}\in B,j=1,2,\cdots,n\},$$

集合中的每一个元素是一个有序 n 元组.

证　对于任意的 f_1，$f_2\in F$，

$$g(f_1)=(f_1(a_1),f_1(a_2),\cdots,f_1(a_n)),$$
$$g(f_2)=(f_2(a_1),f_2(a_2),\cdots,f_2(a_n)).$$

若 $f_1\neq f_2$，则至少存在一个整数 $i(1\leqslant i\leqslant n)$，使得 $f_1(a_i)\neq f_2(a_i)$，因此 $g(f_1)\neq g(f_2)$，故 g 是内射.

对于任意的 $(b_{i_1},b_{i_2},\cdots,b_{i_n})\in B^n$，定义函数 $f:A\to B$，使得 $f(a_1)=b_{i_1}$，$f(a_2)=b_{i_2}$，$\cdots$，$f(a_n)=b_{i_n}$，显然 $f\in F$，且 $g(f)=(b_{i_1},b_{i_2},\cdots,b_{i_n})$，因此 g 是一个满射.

由上证得 $g:F\to B^n$ 是一个双射.

例 3-28 设 A 和 B 都是有限集，$\#A=n$，$\#B=m$，试问由 A 到 B 存在多少个不同的内射？存在多少个不同的双射？

解 若要使函数 $f:A\to B$ 成为内射，必须 $\#A\leqslant\#B$，即 $n\leqslant m$. 否则由 A 到 B 不可能存在内射. 当 $n\leqslant m$ 时，由 A 到 B 可定义 $A_m^n=\dfrac{m!}{(m-n)!}$ 个不同的内射. 此即为从 B 的 m 个元素中取出 n 个元素的排列数.

若要使函数 $f:A\to B$ 成为双射，必须 $\#A=\#B$，即 $n=m$. 否则由 A 到 B 不可能存在双射. 当 $n=m$ 时，由 A 到 B 可定义 $A_m^m=m!$ 个不同的双射. 此即为 B 中 m 个元素的全排列数.

例 3-29 设 A 和 B 都是有限集，且 $\#A=\#B=n$，试证明由 A 到 B 的函数，如果它是内射，则它必是满射. 反之亦真.

证 (反证法)已知 $f:A\to B$ 是内射，假设 f 不是满射，则 B 中至少有一个元素没有像源，即集合 A 中的元素至多只有 $n-1$ 个像，但 $\#A=n$，所以 A 中至少有两个元素对应同一个像，这与 f 是内射相矛盾. 故 f 是满射.

反之，已知 $f:A\to B$ 是满射，假设 f 不是内射，则 A 中至少有两个元素对应同一个像，即 A 在 B 中至多有 $n-1$ 个像，这与 f 是满射相矛盾. 故 f 是内射.

例 3-30 设有函数 $f:A\to B$ 和 $g:C\to D$，定义函数 $h:A\times C\to B\times D$，使得 $h(a,c)=(f(a),g(c))$，试证明当且仅当 f,g 皆为双射时 h 为双射.

证 设 f 和 g 都是双射. 对于任意的 (a_1,c_1) 和 (a_2,c_2)，若 $(a_1,c_1)\neq(a_2,c_2)$，则 $a_1\neq a_2$ 和 $c_1\neq c_2$ 至少有一式成立，因为 f 和 g 都是内射，所以 $f(a_1)\neq f(a_2)$ 和 $g(c_1)\neq g(c_2)$ 至少有一式成立. 因此 $(f(a_1),g(c_1))\neq(f(a_2),g(c_2))$，由函数 h 的定义，即有 $h(a_1,c_1)\neq h(a_2,c_2)$，故 h 是内射.

又对于任意的 $(b,d)\in B\times D$，因为 f 和 g 都是满射，所以必

存在 $a\in A, c\in C$，使得 $f(a)=b, g(c)=d$，因此 $h(a,c)=(b,d)$，故 h 是满射.

由上证得 h 是双射.

反之，设 h 是双射. 对于任意的 $a_1, a_2\in A$，若 $a_1\neq a_2$，则对于任意的 $c\in C$，$(a_1,c)\neq(a_2,c)$，因为 h 是内射，所以 $h(a_1,c)\neq h(a_2,c)$，即 $(f(a_1),g(c))\neq(f(a_2),g(c))$，由 $g(c)=g(c)$，必有 $f(a_1)\neq f(a_2)$，因此 f 是内射.

类似地可以证明 g 是内射.

对于任意 $b\in B$ 和任意的 $d\in D$，$(b,d)\in B\times D$，因为 h 为满射，所以必存在 $(a,c)\in A\times C$，使得 $h(a,c)=(b,d)$，也就是说存在 $a\in A$，使 $f(a)=b$，存在 $c\in C$，使 $g(c)=d$，因此 f 和 g 都是满射.

由上证得 f 和 g 都是双射.

例 3-31 设 f 是由 A 到 B 的函数，$\#A>\#B$.

(1) 当 $\#A$ 除以 $\#B$ 时，设 i 是商，r 是余数，证明

$\left\lceil\frac{\#A}{\#B}\right\rceil=\begin{cases}i+1, & 若\ r\neq 0;\\ i, & 若\ r=0\end{cases}$（$\lceil x\rceil$ 表示不小于 x 的最小整数）.

(2) 证明在 A 中存在 j 个元素 $a_1, a_2, \cdots, a_j$，$j=\left\lceil\frac{\#A}{\#B}\right\rceil$，使得

$$f(a_1)=f(a_2)=\cdots=f(a_j).$$

证 (1) 由题设 $\#A=\#B\cdot i+r$，$(0\leqslant r<\#B)$

因此
$$\frac{\#A}{\#B}=i+\frac{r}{\#B}.\quad\left(0\leqslant\frac{r}{\#B}<1\right)$$

若 $r\neq 0$，则有 $0<\frac{r}{\#B}<1$，于是 $i<\frac{\#A}{\#B}<i+1$

因而有 $\left\lceil\frac{\#A}{\#B}\right\rceil=i+1$，若 $r=0$，则有 $\frac{r}{\#B}=0$，于是 $\frac{\#A}{\#B}=i$，

因此
$$\left\lceil\frac{\#A}{\#B}\right\rceil=i.$$

(2) (用反证法)

假设结论不成立，即假设对于 A 中任意 $j=\left\lceil\frac{\#A}{\#B}\right\rceil$ 个元素 a_1, $a_2, \cdots, a_j$，$f(a_1)=f(a_2)=\cdots=f(a_j)$ 均不成立. 于是 B 中任一元素

b,最多只有 $j-1$ 个像源,因此 A 中最多只有$(j-1)\cdot\#B$ 个元素.即$\#A\leqslant(j-1)\cdot\#B$,即

$$\frac{\#A}{\#B}\leqslant j-1,$$

因此

$$\left\lceil\frac{\#A}{\#B}\right\rceil\leqslant j-1.$$

于是有 $j\leqslant j-1$,矛盾.因此证得结论成立.

例 3-32 设有函数 $f:A\to B,g:B\to C,h:C\to A$,且 hgf 和 gfh 是满射,fhg 是内射,试证明 g,f、h 都是双射.

分析 做此题之前,应该注意到以下几个有关的结论.

(1) 根据复合函数的定义,

hgf 是一由 A 到 A 的函数;

gfh 是一由 C 到 C 的函数;

fhg 是一由 B 到 B 的函数.

(2) 函数的复合运算满足结合律,因此复合函数

$$hgf=h(gf)=(hg)f,$$

即 hgf 既可看作是函数 gf 与 h 的复合,也可看作是函数 f 与 hg 的复合.其它两个复合函数也有类似的结论.

(3) 由函数 f 和 g 的性质可推出 gf 的性质,反之由 gf 的性质可部分地推出 f 和 g 的性质.

(4) 若函数 $f:A\to B$ 是双射,则它存在逆函数 $f^{-1}:B\to A$,f^{-1} 也是双射,并且 $f\cdot f^{-1}=I_B$,$f^{-1}\cdot f=I_A$.

如果熟悉以上四条,那么此题的证明就并不困难.

证 因为 $hgf=(hg)f=h(gf)$是满射,所以 hg 和 h 均是满射.

因为 $gfh=g(fh)=(gf)h$ 是满射,所以 g 和 gf 均是满射.

因为 $fhg=f(hg)=(fh)g$ 是内射,所以 hg 和 g 均是内射.

因此 g 是双射,hg 也是双射.于是 hg 的逆函数$(hg)^{-1}:A\to B$ 也是双射.又

$$(hg)^{-1}\cdot(hgf)=((hg)^{-1}(hg))f=I_B\cdot f=f,$$

式中$(hg)^{-1}$和 hgf 均是满射，所以 f 是满射. 又

$$(fhg)\cdot(hg)^{-1}=f((hg)\cdot(hg)^{-1})=f\cdot I_A=f,$$

式中 fhg 和$(hg)^{-1}$均是内射，所以 f 是内射.

因此　　f 是双射.

因为 g 和 f 均是双射，所以 g^{-1}和 f^{-1}也是双射，于是

$$f^{-1}(fhg)g^{-1}=(f^{-1}f)\cdot h(gg^{-1})=I_AhI_c=h.$$

由 f^{-1}、fhg 和 g^{-1}均是内射，所以 h 也是内射. 因此 h 是双射.

例 3-33　设有函数 $f:A\to B$，定义函数 $g:2^B\to 2^A$，使得对于任一 $S\in 2^B$，有

$$g(S)=\{a\,|\,a\in A\text{ 且 }f(a)\in S\},$$

试问　(1) 当 f 是内射时，g 是否满射?

(2) 当 f 不是内射时，g 是否一定不是满射?

解　(1) 当 f 是内射时，g 是满射.

为了确定在题设条件下，g 是否满射，我们可考察集合 2^A 中任一元素 H，看它在 g 作用下是否一定有像源. 这里要注意的是 $H\in 2^A$，即 $H\subseteq A$，是 A 的任一子集.

另外，符号 $g(S)$中的 $S\in 2^B$，即 S 是 B 的子集，根据 $g(S)$的定义，$g(S)$是 S 中所有元素在 f 作用下的像源的集合.

下面给出这一结论的证明.

证　对任一 $H\in 2^A$，设 $H\neq\varnothing$，并令

$$S=f(H)=\{b\,|\,b\in B,\text{存在 }a\in H\text{ 使得 }f(a)=b\},$$

即 S 是 H 中所有元素在 f 作用下的像的集合. 也就是说，对于任一 $b\in S$，必有 $a\in H$，使 $f(a)=b$，且因为 f 是内射，所以对于 A 中任一元素 $a'\notin H$，有 $f(a')\neq b$. 因此必有 $g(S)=H$. 即 S 是 H 在 g 作用下的像源.

因为 $g(\varnothing)=\varnothing$，所以 2^A 中的元素$\varnothing$也有像源.

由上证得，g 是满射.

(2) 当 f 不是内射时，g 一定不是满射.

证 若 f 不是内射，则必存在元素 $a_i,a_j\in A,a_i\neq a_j$，但 $f(a_i)=f(a_j)=b$，由 $g(S)$ 的定义，$\{a_i\}$ 和 $\{a_j\}$ 在 g 作用下，在 2^B 中均不存在像源. 故 g 不是满射.

为了理解上述结论，我们通过下面两个例子帮助读者建立一些直观的认识.

例 3-34 设 $A=\{a_1,a_2\}$，$B=\{b_1,b_2,b_3\}$，函数 $f_1:A\to B$ 的定义如图 3-6 所示.

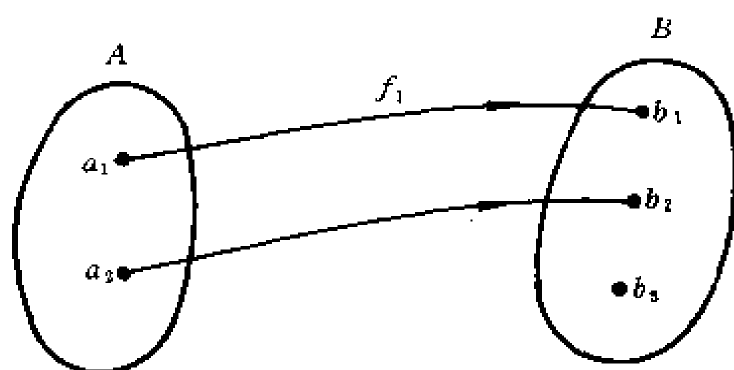


图 3-6

相应的函数 $g_1:2^B\to 2^A$ 如图 3-7 所示.

因为 f_1 是内射，所以 g_1 是满射.

例 3-35 设 $A=\{a_1,a_2,a_3\}$，$B=\{b_1,b_2,b_3\}$，函数 $f_2:A\to B$ 的定义如图 3-8 所示.

相应的函数 $g_2:2^B\to 2^A$ 如图 3-9 所示.

因为 f_2 不是内射，所以 g_2 不是满射.

例 3-36 设有集合 A、B、C 和 D，若 $A\sim B$，$C\sim D$，试证明 $A\times C\sim B\times D$.

证 因为 $A\sim B$，即集合 A 与 B 同基，所以存在双射函数 $f:A\to B$. 又因为 $C\sim D$，所以存在双射函数 $g:C\to D$.

现定义函数 $h:A\times C\to B\times D$，使得 $h(a,c)=(f(a),g(c))$. 根据例 3-29 的结论，h 也是一个双射，因此 $A\times C\sim B\times D$.

例 3-37 证明任一无限集都包含一个与它自身等势的真子

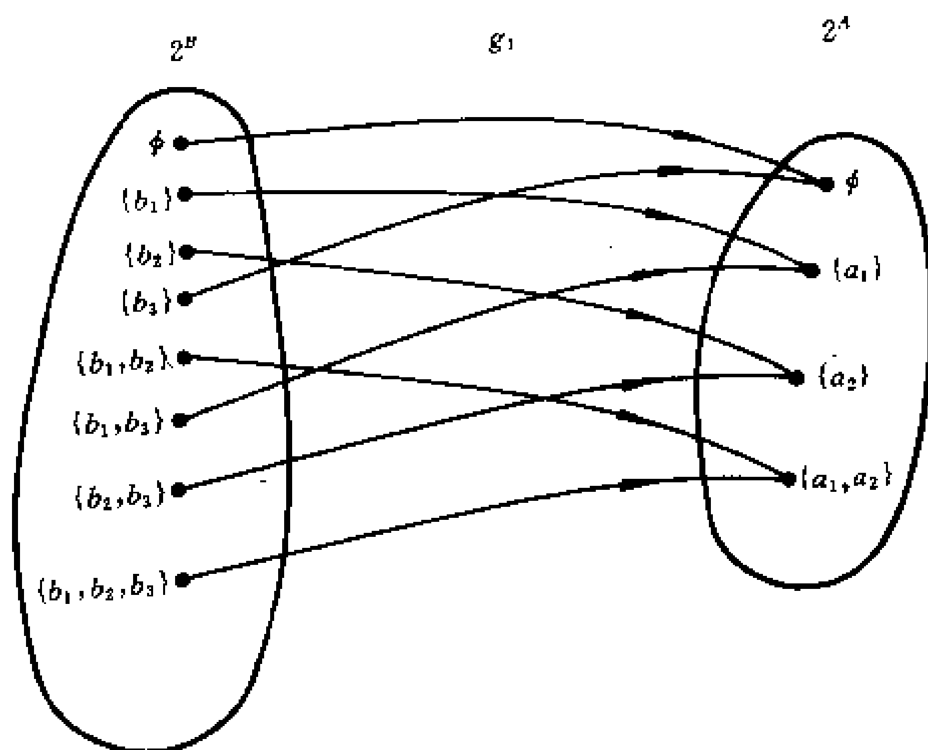


图 3-7

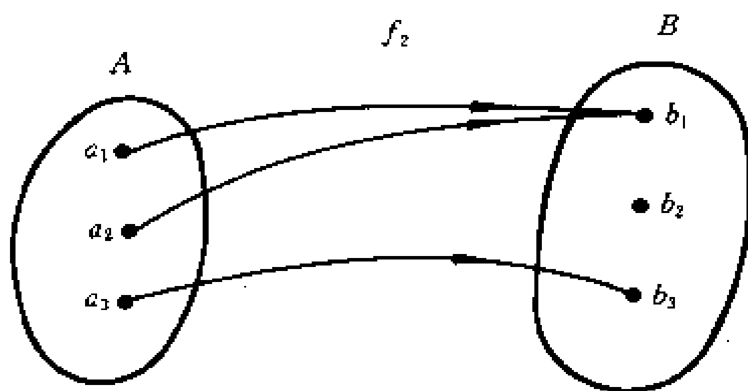


图 3-8

集.

分析 设 A 是一个无限集,此题的要求是要找出 A 的一个真子集,使这个真子集与 A 之间存在双射. 为此我们利用"任一无限集必包含一可数子集"这一性质.

证 设 A 为一无限集,则 A 必包含一可数子集 $M=\{a_{i_1},a_{i_2},\cdots,a_{i_n},\cdots\}$,令 $B=A-M$,在 A 中取出一真子集 $S=\{a_{i_2},a_{i_3},\cdots,$

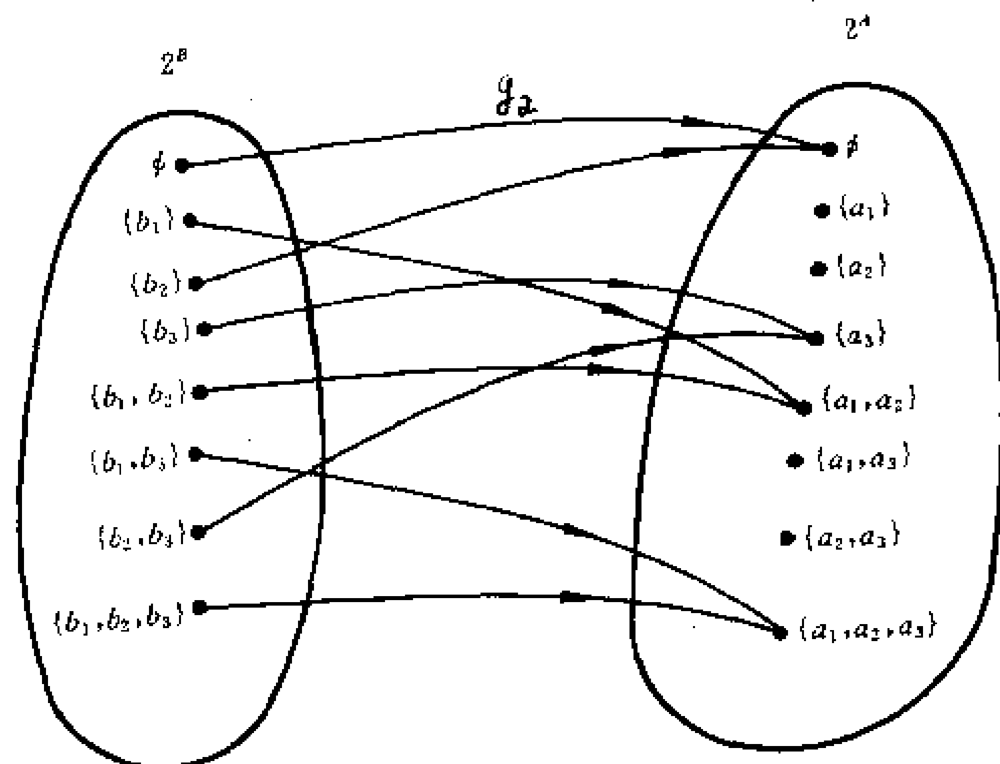


图 3-9

$a_{i_n},\cdots\}\cup B$(即 $S=A-\{a_1\}$),定义函数 $f:A\to S$,使得

$$f(a_{i_j})=f(a_{i_{j+1}})\quad (j=1,2,\cdots)$$

$$f(b)=b\qquad\qquad \text{对任意 } b\in B$$

显然 f 是一由 A 到 S 的双射.

A. 解题思路与方法

由第二章的例 2-31 知道,对于集合 A 上的两个关系 ρ_1 和 ρ_2,若 ρ_1 和 ρ_2 都是对称的,复合关系 $\rho_1\rho_2$ 不一定是对称的;若 ρ_1 和 ρ_2 都是可传递的,$\rho_1\rho_2$ 不一定是可传递的.因此若 ρ_1 和 ρ_2 都是等价关系,$\rho_1\rho_2$ 不一定是等价关系.

例如　设 $A=\{a,b,c\}$,A 上的关系

$$\rho_1=\{(a,a),(b,b),(c,c),(a,b),(b,a)\},$$

$$\rho_2=\{(a,a),(b,b),(c,c),(b,c),(c,b)\}.$$

显然，ρ_1 和 ρ_2 都是等价关系，但 $\rho_1\rho_2$ 不是等价关系. 因为根据复合关系的定义，$(a,c)\in\rho_1\rho_2$，但$(c,a)\notin\rho_1\rho_2$.

那么在什么样的情形下，$\rho_1\rho_2$ 会是等价关系呢？下例给出它成立的一个充要条件.

例 A-1 设 ρ_1 和 ρ_2 是 A 上的等价关系. 试证明当且仅当 $\rho_1\rho_2=\rho_2\rho_1$，$\rho_1\rho_2$ 是 A 上的等价关系.

证 必要性 设 $\rho_1\rho_2$ 是 A 上的等价关系. 若$(a,b)\in\rho_1\rho_2$，则$(b,a)\in\rho_1\rho_2$，于是存在 $c\in A$ 使$(b,c)\in\rho_1$，$(c,a)\in\rho_2$，因此$(c,b)\in\rho_1$，$(a,c)\in\rho_2$，因而$(a,b)\in\rho_2\rho_1$，故 $\rho_1\rho_2\subseteq\rho_2\rho_1$.

若$(a,b)\in\rho_2\rho_1$，则存在 $c'\in A$ 使$(a,c')\in\rho_2$，$(c',b)\in\rho_1$，于是$(b,c')\in\rho_1$，$(c',a)\in\rho_2$，因此$(b,a)\in\rho_1\rho_2$，由 $\rho_1\rho_2$ 的对称性又有$(a,b)\in\rho_1\rho_2$，因此 $\rho_2\rho_1\subseteq\rho_1\rho_2$，由上知 $\rho_1\rho_2=\rho_2\rho_1$.

充分性 设 $\rho_1\rho_2=\rho_2\rho_1$，对于任意的 $a\in A$，因为$(a,a)\in\rho_1$，$(a,a)\in\rho_2$，所以$(a,a)\in\rho_1\rho_2$，因此 $\rho_1\rho_2$ 自反.

对于任意的 $a,b\in A$，若$(a,b)\in\rho_1\rho_2$，则存在 $c\in A$ 使$(a,c)\in\rho_1$，$(c,b)\in\rho_2$，于是$(b,c)\in\rho_2$，$(c,a)\in\rho_1$，因此$(b,a)\in\rho_2\rho_1$. 因为 $\rho_1\rho_2=\rho_2\rho_1$，所以$(b,a)\in\rho_1\rho_2$，故 $\rho_1\rho_2$ 是对称的.

对于任意的 $a,b,c\in A$，若$(a,b)\in\rho_1\rho_2$，$(b,c)\in\rho_1\rho_2$，则有$(b,c)\in\rho_2\rho_1$. 于是存在 $d,e\in A$，使

$$(a,d)\in\rho_1,(d,b)\in\rho_2,(b,e)\in\rho_2,(e,c)\in\rho_1,$$

由 ρ_2 的可传递性有$(a,d)\in\rho_1$，$(d,e)\in\rho_2$，$(e,c)\in\rho_1$，于是有$(d,c)\in\rho_2\rho_1$，因此$(d,c)\in\rho_1\rho_2$，故必存在 $f\in A$，使

$$(d,f)\in\rho_1,(f,c)\in\rho_2,$$

由 ρ_1 的可传递性有$(a,f)\in\rho_1$，又因为$(f,c)\in\rho_2$，所以$(a,c)\in\rho_1\rho_2$. 故 $\rho_1\rho_2$ 是可传递的. 由上知 $\rho_1\rho_2$ 是 A 上的等价关系.

由例 2-33 知道，如果 ρ_1 和 ρ_2 都是集合 A 上的等价关系，$\rho_1\cup\rho_2$不一定是 A 上的等价关系. 那么在什么样的情形下，$\rho_1\cup\rho_2$ 会是等价关系呢？下例给出它成立的一个充分条件.

例 A-2 设 ρ_1 和 ρ_2 都是集合 A 上的等价关系，$\rho_1\rho_2\subseteq\rho_2$，试证

明 $\rho_1 \cup \rho_2$ 是 A 上的等价关系.

分析　在例 2-33 中已经证明了,若 ρ_1 和 ρ_2 是 A 上的等价关系,则 $\rho_1 \cup \rho_2$ 是 A 上的自反和对称的关系. 因此在本例中,只要利用新添加的条件 $\rho_1\rho_2 \subseteq \rho_2$,证明 $\rho_1 \cup \rho_2$ 具有可传递性即可.

证　对于任意的 $a,b,c \in A$,若 $(a,b) \in \rho_1 \cup \rho_2$,$(b,c) \in \rho_1 \cup \rho_2$,则 $(a,b) \in \rho_1$ 或 $(a,b) \in \rho_2$.

若 $(a,b) \in \rho_1$,则由 $(b,b) \in \rho_2$,可得 $(a,b) \in \rho_1\rho_2$,因为 $\rho_1\rho_2 \subseteq \rho_2$,所以 $(a,b) \in \rho_2$.

类似地可以证明 $(b,c) \in \rho_2$.

于是,由 (a,b),$(b,c) \in \rho_2$ 和 ρ_2 的可传递性,得 $(a,c) \in \rho_2$. 因此 $(a,c) \in \rho_1 \cup \rho_2$. 故 $\rho_1 \cup \rho_2$ 是可传递的.

但是上述条件并不是必要条件. 举下例说明之.

例如,设 $A=\{1,2,3,4\}$,A 上的关系

$$\rho_1=\{(1,1),(2,2),(3,3),(4,4),(1,3),(3,1),(1,4),(4,1),(3,4),(4,3)\},$$

$$\rho_2=\{(1,1),(2,2),(3,3),(4,4),(3,4),(4,3)\}$$

均是等价关系,且 $\rho_1 \cup \rho_2 = \rho_1$ 也是等价关系. 但 $\rho_1\rho_2 \not\subseteq \rho_2$.

若 ρ 是集合 A 上的等价关系,那么 ρ 的等价类的个数常称为 ρ 的秩.

在例 2-33 中我们曾证明了,若 ρ_1 和 ρ_2 都是集合 A 上的等价关系,则 $\rho_1 \cap \rho_2$ 也是 A 上的等价关系. 进一步我们有下面的结论.

例 A-3　设 ρ_1 和 ρ_2 是集合 A 上分别有秩 r_1 和 r_2 的等价关系,试证明等价关系 $\rho_1 \cap \rho_2$ 的秩至多为 $r_1 \cdot r_2$.

分析　我们知道,集合 A 上等价关系 ρ 的所有等价类构成 A 的一个分划,每一个等价类便是该分划的一个分划块. 而且我们知道,集合 A 上的等价关系与 A 的分划一一对应,因此在描述集 A 上的一个等价关系时,我们常用与它对应的等价分划来简洁地表示它.

由题设条件可知,ρ_1 所导致的 A 的分划 $\Pi_{\rho_1}^A$ 有 r_1 个分划块,ρ_2

所导致的 A 的分划 $\Pi^A_{\rho_2}$ 有 r_2 个分划块，题目要求我们证明 $\rho_1 \cap \rho_2$ 所导致的分划块至多为 $r_1 \cdot r_2$ 个.

设 $\Pi^A_{\rho_1}=\{A_1,A_2,\cdots,A_{r_1}\}$，$\Pi^A_{\rho_2}=\{B_1,B_2,\cdots,B_{r_2}\}$，于是当 $i\neq j$ 时，因为 A_i 与 A_j 是同一个分划的两个不同的分划块，所以 $A_i\cap A_j=\varnothing$，同样的道理，$B_i\cap B_j=\varnothing$. 但对于任意的 $i,j(1\leqslant i\leqslant r_1,1\leqslant j\leqslant r_2)$，$A_i\cap B_j$ 却可能不为 $\varnothing$，因此形为 $A_i\cap B_j$ 的交集有 $r_1\cdot r_2$ 个，其中不为 $\varnothing$ 的交集的个数至多为 $r_1\cdot r_2$ 个.

而且我们注意到，对于任意两个不同的交集 $A_i\cap B_j$ 与 $A_k\cap B_l(i\neq k$ 或 $j\neq l)$，$(A_i\cap B_j)\cap(A_k\cap B_l)=\varnothing$，因此，所有这样的非空交集 $(A_i\cap B_j)$ 有可能构成集合 A 的分划. 这一分划可能与等价关系 $\rho_1\cap\rho_2$ 对应.

以上只是我们的分析和推测. 下面我们以此为目标来证明，以证实我们推测的结论是否正确. 为此，我们假设分划 $\Pi^A_{\rho_1\cap\rho_2}=\{c_t\}_{t\in k}$，如果我们能证明每一个分划块 c_t 均和某一个交集 $A_i\cap B_j$ 相等，则 $\Pi^A_{\rho_1\cap\rho_2}$ 的分划块就是有限个，且个数 $\leqslant r_1\cdot r_2$.

证 设 $\Pi^A_{\rho_1}=\{A_1,A_2,\cdots,A_{r_1}\}$，$\Pi^A_{\rho_2}=\{B_1,B_2,\cdots,B_{r_2}\}$，$\Pi^A_{\rho_1\cap\rho_2}=\{c_t\}_{t\in k}$. 任取一 $c_t\in\Pi^A_{\rho_1\cap\rho_2}$，由分划的定义 c_t 非空，因此必存在一元素 $x\in C_t$. 由于 $\Pi^A_{\rho_1}$ 和 $\Pi^A_{\rho_2}$ 也是 A 的分划，因此有 $A_i(1\leqslant i\leqslant r_1)$ 和 $B_j(1\leqslant j\leqslant r_2)$ 存在，使得 $x\in A_i$，$x\in B_j$，于是 $x\in A_i\cap B_j$. 下面证明 $c_t=A_i\cap B_j$.

任取 $y\in C_t$，因为 $(x,y)\in\rho_1\cap\rho_2$，所以 $(x,y)\in\rho_1$ 且 $(x,y)\in\rho_2$，因此有 $y\in A_i$ 且 $y\in B_j$，于是 $y\in A_i\cap B_j$，故 $C_t\subseteq A_i\cap B_j$.

反之，任取 $z\in A_i\cap B_j$，则 $z\in A_i$ 且 $z\in B_j$，所以 $(x,z)\in\rho_1$，$(x,z)\in\rho_2$，因此 $(x,z)\in\rho_1\cap\rho_2$，由 $x\in C_t$，所以 $z\in C_t$，故 $A_i\cap B_j\subseteq C_t$.

由此可知任一 C_t 必等于某一个 $A_i\cap B_j$，然而形为 $A_i\cap B_j(1\leqslant i\leqslant r_1,1\leqslant j\leqslant r_2)$ 的非空集合至多只有 $r_1\cdot r_2$ 个，所以等价关系 $\rho_1\cap\rho_2$ 的秩至多为 $r_1\cdot r_2$.

例 A-3 的结论说明 $\rho_1\cap\rho_2$ 所导致的 A 的分划是 ρ_1 所导致的

A 的分划的细分，也是 ρ_2 所导致的 A 的分划的细分.

利用例 2-35 的结论，我们可以给出例 A-3 的另一证明方法.

证法二 设$\Pi^A_{\rho_1}=\{[a_1]_{\rho_1},[a_2]_{\rho_1},\cdots,[a_{r_1}]_{\rho_1}\}$,

$\Pi^A_{\rho_2}=\{[b_1]_{\rho_2},[b_2]_{\rho_2},\cdots,[b_{r_2}]_{\rho_2}\}$,

$\Pi^A_{\rho_1\cap\rho_2}=\{[c_t]_{\rho_1\cap\rho_2}\mid t\in K\}$.

显然 $\rho_1\cap\rho_2\subseteq\rho_1$，$\rho_1\cap\rho_2\subseteq\rho_2$，由例 2-35 的结论，对于任一$[c_t]_{\rho_1\cap\rho_2}\in\Pi^A_{\rho_1\cap\rho_2}$，必存在正整数 i 和 $j(1\leqslant i\leqslant r_1,1\leqslant j\leqslant r_2)$使得

$$[c_t]_{\rho_1\cap\rho_2}\subseteq[a_i]_{\rho_1},[c_t]_{\rho_1\cap\rho_2}\subseteq[b_j]_{\rho_2},$$

因此
$$[c_t]_{\rho_1\cap\rho_2}\subseteq[a_i]_{\rho_1}\cap[b_j]_{\rho_2}.$$

现假设 $\Pi^A_{\rho_1\cap\rho_2}$中有两个等价类$[c_t]_{\rho_1\cap\rho_2}$与$[c_h]_{\rho_1\cap\rho_2}$都包含于$[a_i]_{\rho_1}\cap[b_j]_{\rho_2}$之中，即

$$[c_t]_{\rho_1\cap\rho_2}\subseteq[a_i]_{\rho_1}\cap[b_j]_{\rho_2},[c_h]_{\rho_1\cap\rho_2}\subseteq[a_i]_{\rho_1}\cap[b_j]_{\rho_2}.$$

则 $(c_t,a_i)\in\rho_1,(c_h,a_i)\in\rho_1$，因此$(c_t,c_h)\in\rho_1$,

又 $(c_t,b_j)\in\rho_2,(c_h,b_j)\in\rho_2$，因此$(c_t,c_h)\in\rho_2$,

于是$(c_t,c_h)\in\rho_1\cap\rho_2$，因而有$[c_t]_{\rho_1\cap\rho_2}=[c_h]_{\rho_1\cap\rho_2}$. 这说明 $\Pi^A_{\rho_1\cap\rho_2}$中只有唯一的一个等价类包含于$[a_i]_{\rho_1}\cap[b_j]_{\rho_2}$之中. 然而形如$[a_i]_{\rho_1}\cap[b_j]_{\rho_2}$的非空集合至多只有 $r_1\cdot r_2$ 个，因此 $\rho_1\cap\rho_2$ 的秩至多是 $r_1\cdot r_2$.

例 A-4 设 R 为集合 A 上的自反和可传递的关系.

(1) 你能否根据 R，在 A 上再定义一个关系 ρ，使 ρ 成为一个等价关系?

(2) 又若在 A/ρ 上定义关系 R'，使得当且仅当$(x,y)\in R$ 时，$([x]_\rho,[y]_\rho)\in R'$，试证明 R' 是 A/ρ 上的编序关系.

解 (1) 由题设 R 已具有自反性和传递性，但 R 不一定具有对称性. 也就是说，对于任意序偶$(a,b)\in R$，(b,a)可能不属于 R. 那么将序偶(b,a)添加到 R 中去不就可以使 R 满足对称性吗?

为此令 $\rho=R\cup\tilde{R}$，这里 $\tilde{R}$ 是 R 的逆关系. ρ 仍具有自反性是显然的. 对称性也满足，因为对于任意$(a,b)\in\rho$，有$(a,b)\in R$ 或

$(a,b)\in\widetilde{R}$，于是有$(b,a)\in\widetilde{R}$或$(b,a)\in R$，因此$(b,a)\in\rho$. 但R的传递性是否会因为添加了某些序偶而遭到破坏呢？为此我们看下面的例子.

例如　设$A=\{1,2,3\}$，A上的关系，

$$R=\{(1,1),(2,2),(3,3),(1,2),(3,2)\}$$

是自反的和可传递的. R的逆关系

$$\widetilde{R}=\{(1,1),(2,2),(3,3),(2,1),(2,3)\},$$

于是

$$R\cup\widetilde{R}=\{(1,1),(2,2),(3,3),(1,2),(3,2),(2,1),(2,3)\}.$$

显然$R\cup\widetilde{R}$是自反的，也是对称的，但却是不可传递的. 因为$(1,2),(2,3)\in R\cup\widetilde{R}$，但$(1,3)\notin R\cup\widetilde{R}$. 因此用上述方式来定义$\rho$不能满足题目的要求.

注意到集合A上任一关系ρ，不论它是否具有可传递性，它的传递闭包ρ^+一定是可传递的. 因此可否将ρ定义为$(R\cup\widetilde{R})^+$呢？

解法一　定义A上的关系$\rho=(R\cup\widetilde{R})^+$. 下面证明$\rho$是$A$上的等价关系.

对于任意$a\in A$，有$(a,a)\in R$，所以$(a,a)\in R\cup\widetilde{R}$，因此$(a,a)\in\rho$，故$\rho$是自反的.

对于任意$a,b\in A$，若$(a,b)\in\rho$，则必存在正整数r，使得$(a,b)\in(R\cup\widetilde{R})^r$，于是存在元素$a_{i_1},a_{i_2},\cdots,a_{i_{r-1}}\in A$，使得

$$a(R\cup\widetilde{R})a_{i_1},a_{i_1}(R\cup\widetilde{R})a_{i_2},\cdots,a_{i_{r-1}}(R\cup\widetilde{R})b$$

因为$R\cup\widetilde{R}$是对称的，所以有

$$b(R\cup\widetilde{R})a_{i_{r-1}},\cdots,a_{i_2}(R\cup\widetilde{R})a_{i_1},a_{i_1}(R\cup\widetilde{R})a$$

于是$b(R\cup\widetilde{R})^r a$，即$(b,a)\in(R\cup\widetilde{R})^r$，因而$(b,a)\in\rho$，故$\rho$是对称的.

由传递闭包的性质，ρ是可传递的.

由上可知ρ是A上的等价关系.

对于任意$(a,b)\in R$，(b,a)可能不属于R，这一现象影响了R的对称性，那么在此情形下，我们将序偶(a,b)从R中去掉，仅保

留那些(a,b)与(b,a)均在R中的序偶，不也可以使R具有对称性吗？

为此令$\rho=\{(a,b)\mid(a,b)\in R$且$(b,a)\in R\}$. 即令$\rho=R\cap\widetilde{R}$. 与前面$R\cup\widetilde{R}$不同的是，这样定义的$\rho$仍保持了$R$的可传递性. 下面给出证明.

解法二 定义A上的关系$\rho=R\cap\widetilde{R}$.

对于任意的$a\in A$，因为R自反，所以$(a,a)\in R$，因此$(a,a)\in\widetilde{R}$，于是$(a,a)\in\rho$，故ρ自反.

对于任意$a,b\in A$，若$(a,b)\in\rho$，则$(a,b)\in R$且$(a,b)\in\widetilde{R}$，于是$(b,a)\in\widetilde{R}$且$(b,a)\in R$，因此$(b,a)\in\rho$，故ρ是对称的.

对于任意$a,b,c\in A$，若$(a,b)\in\rho$且$(b,c)\in\rho$，则$(a,b)\in R$，$(b,c)\in R$且$(a,b)\in\widetilde{R}$，$(b,c)\in\widetilde{R}$，由R和$\widetilde{R}$的可传递性，有$(a,c)\in R$且$(a,c)\in\widetilde{R}$，因此$(a,c)\in\rho$，故ρ是可传递的.

由上证得ρ是等价关系.

若令$\rho=R\cdot\widetilde{R}$，利用复合关系和逆关系的性质，可使ρ具有对称性. 因为对于任意的$a,b\in A$若$(a,b)\in\rho$，则必存在$c\in A$，使$(a,c)\in R$，$(c,b)\in\widetilde{R}$，于是$(b,c)\in R$，$(c,a)\in\widetilde{R}$，因此$(b,a)\in R\cdot\widetilde{R}$，即$(b,a)\in\rho$，故$\rho$是对称的. ρ的自反性是显然的. 但可惜的是ρ可能不具有传递性.

例如，设$A=\{1,2,3,4,5\}$，A上的关系

$$R=\{(1,1),(2,2),(3,3),(4,4),(5,5),(1,4),(2,5),(2,4),(3,5)\},$$

则

$$\widetilde{R}=\{(1,1),(2,2),(3,3),(4,4),(5,5),(4,1),(5,2),(4,2),(5,3)\},$$

$$R\cdot\widetilde{R}=\{(1,1),(2,2),(3,3),(4,4),(5,5),(4,1),(5,2),(4,2),(5,3),(1,2),(2,3),(2,1),(3,2),(1,4),(2,5),(2,4),(3,5)\}.$$

在这里R是自反和可传递的. $R\cdot\widetilde{R}$是自反和对称的，但$R\cdot\widetilde{R}$不可传递. 因为$(1,2),(2,3)\in R\cdot\widetilde{R}$，但$(1,3)\notin R\cdot\widetilde{R}$. 因此

用上述方式定义的 ρ，不能满足题目的要求. 为使 ρ 具有可传递性，我们可令 $\rho=(R\cdot\widetilde{R})^{+}$.

解法三 定义 A 上的关系 $\rho=(R\cdot\widetilde{R})^{+}$. 下面证明 ρ 是 A 上的等价关系.

对于任意的 $a\in A$，有 $(a,a)\in R$，$(a,a)\in\widetilde{R}$，所以 $(a,a)\in R\cdot\widetilde{R}$，因此 $(a,a)\in\rho$，故 ρ 是自反的.

对于任意 $a,b\in A$，若 $(a,b)\in\rho$，则必存在某正整数 r，使得 $(a,b)\in(R\cdot\widetilde{R})^{r}$，于是存在元素 $a_{i_1},a_{i_2},\cdots,a_{i_{r-1}}\in A$，使得

$$a(R\cdot\widetilde{R})a_{i_1},a_{i_1}(R\cdot\widetilde{R})a_{i_2},\cdots,a_{i_{r-1}}(R\cdot\widetilde{R})b$$

因为 $R\cdot\widetilde{R}$ 是对称的，所以有

$$b(R\cdot\widetilde{R})a_{i_{r-1}},a_{i_{r-1}}(R\cdot\widetilde{R})a_{i_{r-2}},\cdots,a_{i_2}(R\cdot\widetilde{R})a_{i_1},a_{i_1}(R\cdot\widetilde{R})a.$$

于是 $b(R\cdot\widetilde{R})^{r}a$，因而 $(b,a)\in\rho$，故 ρ 是对称的.

由传递闭包的性质，ρ 是可传递的.

由上证得 ρ 是 A 上的等价关系.

证 (2)

由解法一，$\rho=(R\cup\widetilde{R})^{+}$.

对于任意 $[x]_\rho\in A/\rho$，因为 $(x,x)\in R$，所以 $([x]_\rho,[x]_\rho)\in R'$，因此 R' 是自反的.

对于任意 $[x]_\rho,[y]_\rho\in A/\rho$，若 $([x]_\rho,[y]_\rho)\in R'$ 且 $([y]_\rho,[x]_\rho)\in R'$，则有 $(x,y)\in R$ 且 $(y,x)\in R$，由 $(x,y)\in R$，必有 $(x,y)\in\rho$，因此 $[x]_\rho=[y]_\rho$，故 R' 是反对称的.

对于任意 $[x]_\rho,[y]_\rho,[z]_\rho\in A/\rho$，若 $([x]_\rho,[y]_\rho)\in R'$ 且 $([y]_\rho,[z]_\rho)\in R'$，则 $(x,y)\in R$ 且 $(y,z)\in R$，由 R 的可传递性，必有 $(x,z)\in R$，所以 $([x]_\rho,[z]_\rho)\in R'$，因此 R' 是可传递的.

由上证得 R' 是 A/ρ 上的偏序关系.

由上面的证明我们看出，R' 的自反性和可传递性分别依赖于 R 的自反性和可传递性，只有 R' 的反对称性与 ρ 的定义有关. 因此对于解法二和解法三，我们只给出 R' 的反对称性的证明.

由解法二，$\rho=R\cap\widetilde{R}$.

对于任意$[x]_\rho,[y]_\rho\in A/\rho$，若$([x]_\rho,[y]_\rho)\in R'$且$([y]_\rho,[x]_\rho)\in R'$，则$(x,y)\in R$且$(y,x)\in R$，于是有$(x,y)\in\tilde{R}$，因此$(x,y)\in\rho$，于是$[x]_\rho=[y]_\rho$，故$R'$是反对称的.

由解法三，$\rho=(R\cdot\tilde{R})^+$.

对于任意$[x]_\rho,[y]_\rho\in R'$，若$([x]_\rho,[y]_\rho)\in R'$且$([y]_\rho,[x]_\rho)\in R'$，则有$(x,y)\in R$，又$(y,y)\in\tilde{R}$，所以$(x,y)\in R\cdot\tilde{R}$，因此$(x,y)\in\rho$，于是$[x]_\rho=[y]_\rho$，故$R'$是反对称的.

例 A-5　设A为任意非空集合，$F=\{f\mid f:A\to\{0,1\}\}$，试证明$2^A$与$F$等势.

分析　要证明2^A与F等势，即要证明由2^A到F存在双射. 我们采用构造式证明方法，通过定义一个由2^A到F的双射来证明双射的存在.

证　定义函数$g:2^A\to F$，使得对于任意的$S\in 2^A$，即对于任意$S\subseteq A$，$g(S)=f$，这里函数$f:A\to\{0,1\}$是根据S来定义的，

$$f(a_i)=\begin{cases}0, & 若\ a_i\in S;\\ 1, & 若\ a_i\notin S.\end{cases}$$

g是内射. 其证明如下：

设$S_1,S_2\in 2^A$，$g(S_1)=f_1$，$g(S_2)=f_2$，若$S_1\neq S_2$，则必存在$a_i\in S_1$，但$a_i\notin S_2$，或者存在$a_j\notin S_1$，但$a_j\in S_2$. 不失一般性，假设存在$a_i\in S_1$，但$a_i\notin S_2$，则有$f_1(a_i)=0$，$f_2(a_i)=1$，于是$f_1\neq f_2$，即$g(S_1)\neq g(S_2)$，因此g是一个内射.

g是满射. 其证明如下：

对于任意的$f\in F$，令$S=\{a\mid a\in A 且 f(a)=0\}$，则由$g$的定义可知$g(S)=f$. 因此$g$是一个满射.

因为g是双射，所以2^A与F等势.

例 A-6　设A为任意非空集合，$Z_n=\{0,1,\cdots,n-1\}$，$F=\{f\mid f:Z_n\to A\}$. 试证明存在由F到A^n的双射.

证　定义函数$g:F\to A^n$，使得对于任意$f\in F$，$g(f)=(f(0),f(1),\cdots,f(n-1))$.

对于任意 f_1、$f_2 \in F$，若 $f_1 \neq f_2$，则至少存在一个 $i \in Z_n$，使得 $f_1(i) \neq f_2(i)$，因此 $g(f_1) \neq g(f_2)$，故 g 是内射

对于任一有序 n 元组 $(a_0, a_1, \cdots, a_{n-1}) \in A^n$，定义 $f: Z_n \to A$，使 $f(0)=a_0, f(1)=a_1, \cdots, f(n-1)=a_{n-1}$，则由 g 的定义必有

$$g(f) = (a_0, a_1, \cdots, a_{n-1}).$$

故 g 是满射.

由上证得 g 是双射.

例 A-7 设有集合 A，令 $A^A = \{f \mid f: A \to A\}$，集合 A^A 上的关系 ρ 定义为，对于任意的 $f, g \in A^A$，当且仅当 $R_f = R_g$ 时，$f\rho g$.

(1) 证明 ρ 是 A^A 上的等价关系；

(2) 证明由集合 A^A/ρ 到 $2^A - \{\varnothing\}$ 存在双射.

分析 只要概念清楚，此题的证明并不困难. 关键是在做此题之前，要将题目中各种记号的含义以及相关的概念搞清楚.

$f, g \in A^A$，表示 f 和 g 都是由 A 到 A 的函数. R_f 表示函数 f 的值域. 因此 $R_f = R_g$ 表示函数 f 和 g 的值域是相等的.

若 ρ 是 A^A 上的等价关系，那么 A^A/ρ 表示由 ρ 所导致的集合 A^A 上的等价分划，即 A^A/ρ 是由 ρ 在 A^A 中的所有等价类组成的集合，这一集合也称为集合 A^A 关于等价关系 ρ 的商集.

证 (1) 对于任意 $f \in A^A$，因为 $R_f = R_f$，所以 $f\rho f$，因此 ρ 是自反的.

对于任意 $f, g \in A^A$，若 $f\rho g$，则 $R_f = R_g$，即 $R_g = R_f$，所以 $g\rho f$，因此 ρ 是对称的.

对于任意 f、g，$h \in A^A$，若 $f\rho g$，$g\rho h$，则 $R_f = R_g$，$R_g = R_h$，于是 $R_f = R_h$，因此 $f\rho h$，故 ρ 是可传递的.

由上证得 ρ 是等价关系.

(2) 思路 A^A/ρ 中的元素是形如 $[f]_\rho$ 的等价类，其中 f 是由 A 到 A 的函数，$[f]_\rho$ 是由 A^A 中所有与 f 有相同值域的函数所组成，即

$$[f]_\rho = \{g \mid g: A \to A \text{ 且 } R_g = R_f\}.$$

由于$[f]_\rho$中所有函数都具有相同的值域，因此我们很容易想到，在定义双射$F:A^A/\rho\to 2^A-\{\varnothing\}$时，让每一个等价类$[f]_\rho$与其值域$R_f$对应.

证 定义函数$F:A^A/\rho\to 2^A-\{\varnothing\}$，使得对任意$[f]_\rho\in A^A/\rho$，$F([f]_\rho)=R_f$.

设$[f]_\rho$、$[h]_\rho\in A^A/\rho$且$F([f]_\rho)=F([h]_\rho)$，则$R_f=R_h$，因此$f\rho h$，于是$[f]_\rho=[h]_\rho$. 故F是内射.

又对于任意的$S\in 2^A-\{\varnothing\}$，则$S\subseteq A$且$S\neq\varnothing$，任取一元素$a\in S$，定义函数$f:A\to A$，使得

$$f(x)=\begin{cases}x, & 若\ x\in S;\\ a, & 若\ x\notin S.\end{cases}$$

显然$R_f=S$，因此$F([f]_\rho)=S$，故F是满射.

由上证得$F:A^A/\rho\to 2^A-\{\varnothing\}$是一双射.

例 A-8 设$A^A=\{f\mid f:A\to A\}$，$h\in A^A$. 试证明当且仅当h是满射时，对于任意的$f,g\in A^A$，由$f\cdot h=g\cdot h$，可推得$f=g$.

证 **充分性** 设h是满射，且有$f,g\in A^A$，使得$f\cdot h=g\cdot h$. 对于任意的$b\in A$，必有$a\in A$，使得$h(a)=b$，于是

$$f(b)=f(h(a))=f\cdot h(a);$$
$$g(b)=g(h(a))=g\cdot h(a).$$

因为$f\cdot h=g\cdot h$，所以$f\cdot h(a)=g\cdot h(a)$，此即$f(b)=g(b)$. 由b的任意性，可得$f=g$.

必要性 设对于任意f、$g\in A^A$，由$f\cdot h=g\cdot h$，可推得$f=g$. 又假设h不是满射(反证法)，则必有元素$b\in A$，$b\notin h(A)$. 定义函数$f=I_A$，函数$g:A\to A$，使得

$$g(a)=\begin{cases}a, & 当\ a\in h(A);\\ a_0, & 当\ a\notin h(A).\end{cases}$$

这里a_0是$h(A)$中的某一元素. 于是对于任意的$a\in A$，

$$f\cdot h(a)=f(h(a))=h(a),$$
$$g\cdot h(a)=g(h(a))=h(a)\quad (因为\ h(a)\in h(A)),$$

因此有 $f \cdot h = g \cdot h$，但因 $f(b)=b$，而 $g(b)=a_0$，$a_0 \neq b$，所以 $f \neq g$. 这与题设相矛盾. 故 h 必为满射.

例 A-9 设 R 是集合 A 上的一个关系.

(1) 求 A 上包含 R 的最小等价关系 ρ 的表达式;

(2) 证明 ρ 的最小性;

(3) 以 $A=\{1,2,3,4,5,6\}$，$R=\{(1,2),(1,3),(4,4),(4,5)\}$ 为例验证你的结果.

分析 为使 ρ 包含 R 且满足对称性，必须将 R 的逆关系 $\tilde{R}$ 中的序偶添加到 R 中去，即令 $\rho_1 = R \cup \tilde{R}$. 如使 ρ_1 满足自反性，必须将 I_A 中的序偶添加到 ρ_1 中去，因此令 $\rho_2 = I_A \cup (R \cup \tilde{R})$. 根据例 A-4 的讨论，$R \cup \tilde{R}$ 不一定具有可传递性，为使 ρ_2 具有可传递性，令 $\rho_3 = I_A \cup (R \cup \tilde{R})^+$.

解 (1) $\rho = I_A \cup (R \cup \tilde{R})^+$ 是 A 上包含 R 的最小等价关系.

因为 $I_A \subseteq \rho$，所以 ρ 是自反的.

由例 A-4 的证明，$(R \cup \tilde{R})^+$ 是对称的，因此 ρ 也是对称的.

由传递闭包的性质，$(R \cup \tilde{R})^+$ 是可传递的，因此 ρ 也是可传递的.

(2) 设 S 是 A 上包含 R 的任一等价关系，则 $\rho \subseteq S$. 下面给出这一结论的证明.

首先，由 $R \subseteq S$，可得 $\tilde{R} \subseteq S$. 因为对于任意 $(a,b) \in \tilde{R}$，必有 $(b,a) \in R$，于是 $(b,a) \in S$，由 S 的对称性，又有 $(a,b) \in S$，因此 $\tilde{R} \subseteq S$.

由上可知，$R \cup \tilde{R} \subseteq S$.

设 $(a,b) \in \rho$，则 $(a,b) \in I_A$ 或 $(a,b) \in (R \cup \tilde{R})^+$.

若 $(a,b) \in I_A$，由 S 的自反性，必有 $(a,b) \in S$.

若 $(a,b) \in (R \cup \tilde{R})^+$，则必存在正整数 r，使得 $(a,b) \in (R \cup \tilde{R})^r$，因此必存在元素 $a_{i_1}, a_{i_2}, \cdots, a_{i_{r-1}} \in A$，使得

$$(a, a_{i_1}) \in R \cup \tilde{R}, (a_{i_1}, a_{i_2}) \in R \cup \tilde{R}, \cdots, (a_{i_{r-1}}, b) \in R \cup \tilde{R},$$

因为 $R \cup \tilde{R} \subseteq S$，所以有

$$(a,a_{i_1})\in S,(a_{i_1},a_{i_2})\in S,\cdots,(a_{i_{r-1}},b)\in S,$$

由 S 的传递性，有 $(a,b)\in S$，故 $\rho\subseteq S$. 由此证明了 ρ 的最小性.

(3) 由 $R=\{(1,2),(1,3),(4,4),(4,5)\}$，

则 $\quad \widetilde{R}=\{(2,1),(3,1),(4,4),(5,4)\}$，

$$R\cup\widetilde{R}=\{(1,2),(2,1),(1,3),(3,1),(4,4),(4,5),(5,4)\}.$$

构造 $R\cup\widetilde{R}$ 的关系图，如图 A-1 所示. 根据 $R\cup\widetilde{R}$ 的关系图构造出 $(R\cup\widetilde{R})^+$ 的关系图，如图 A-2 所示. 由此得

$$\begin{aligned}\rho&=I_A\cup(R\cup\widetilde{R})^+\\&=\{(1,1),(2,2),(3,3),(4,4),(5,5),(1,2),(2,1),(1,3),(3,1),(2,3),(3,2),(4,5),(5,4),(6,6)\}.\end{aligned}$$

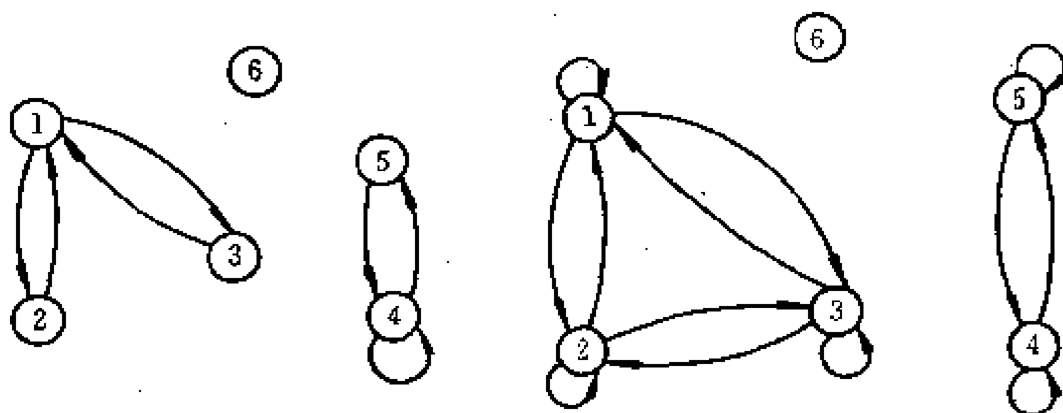


图 A-1 $\quad R\cup\widetilde{R}$ 的关系图 $\qquad$ 图 A-2 $\quad (R\cup\widetilde{R})^+$ 的关系图

显然，ρ 是等价关系，且是包含 R 的最小的等价关系.

例 A-10 设有集合 A、B，试证明由 A 到 B 的一个函数可决定 A 的一个分划；A 的一个分划 Π 可决定由 A 到 Π 的一个函数.

证 设有函数 $f:A\to B$，定义 A 上的关系 ρ_f，使得对于任意的 $a_i,a_j\in A$，当且仅当 $f(a_i)=f(a_j)$ 时，$a_i\rho_f a_j$.

对于任意的 $a\in A$，有 $f(a)=f(a)$，所以 $a\rho_f a$，因此 ρ_f 是自反的.

对于任意 $a_i,a_j\in A$，若 $a_i\rho_f a_j$，则 $f(a_i)=f(a_j)$，即 $f(a_j)=f(a_i)$，所以 $a_j\rho_f a_i$，因此 ρ_f 是对称的.

对于任意 $a_i, a_j, a_k \in A$，若 $a_i \rho_f a_j$，$a_j \rho_f a_k$，则 $f(a_i)=f(a_j)$，$f(a_j)$，$f(a_j)=f(a_k)$，因此 $f(a_i)=f(a_k)$. 于是 $a_i \rho_f a_k$，因此 ρ_f 是可传递的.

由上得 ρ_f 是 A 上的等价关系. 因此有 ρ_f 所导致的集 A 上的等价分划 $\Pi_{\rho_f}^A$.

设 $\Pi=\{A_i\}_{i\in k}$是 A 的一个分划. 于是对于任意 $a\in A$，有且仅有唯一 $A_i(i\in k)$，使得 $a\in A_i$. 定义函数 $g:A\to\Pi$，使得对于任意 $a\in A$，当且仅当 $a\in A_i$ 时，$g(a)=A_i$. 显然该函数 g 是由 A 到 Π 的一个满射.

例 A-11 设有集合 A,B，函数 $f:A\to B$ 是一满射. 试证明存在双射 $g:\Pi_{\rho_f}^A\to B$，且存在满射 $\varphi:A\to\Pi_{\rho_f}^A$使得 $g\cdot\varphi=f$.（ρ_f 的定义和 $\Pi_{\rho_f}^A$的含义在例 A-10 中已给出）

分析 采用构造式的证明方法，恰当地定义函数 $g:\Pi_{\rho_f}^A\to B$ 和 $\varphi:A\to\Pi_{\rho_f}^A$，然后证明这两个函数满足题目所要求的条件.

在证明过程中要注意的是，对于任一等价类$[a]_{\rho_f}\in\Pi_{\rho_f}^A$，$[a]_{\rho_f}$中的每一个元素在 f 作用下的函数值均相等. 即若 $a_i,a_j\in[a]_{\rho_f}$，则 $f(a_i)=f(a_j)=f(a)$.

证 定义函数 $g:\Pi_{\rho_f}^A\to B$，使得对于任意$[a]_{\rho_f}\in\Pi_{\rho_f}^A$，$g([a]_{\rho_f})=f(a)$.

对于任意 $b\in B$，因为 f 是满射，所以必有 $a\in A$，使得 $f(a)=b$，因此 $g([a]_{\rho_f})=f(a)=b$. 这说明对于任意 $b\in B$，必有 $[a]_{\rho_f}\in\Pi_{\rho_f}^A$使 $g([a]_{\rho_f})=b$，所以 g 是满射.

设$[a_i]_{\rho_f}$、$[a_j]_{\rho_f}\in\Pi_{\rho_f}^A$，且$[a_i]_{\rho_f}\neq[a_j]_{\rho_f}$，则 $(a_i,a_j)\notin\rho_f$，因此 $f(a_i)\neq f(a_j)$. 由函数 g 的定义，

$$g([a_i]_{\rho_f})\neq g([a_j]_{\rho_f})$$

因此 g 是内射.

由上证得 g 是双射.

定义函数 $\varphi:A\to\Pi_{\rho_f}^A$，使得对于任意 $a\in A$，$\varphi(a)=[a]_{\rho_f}$.

对于任意$[a_i]_{\rho_f} \in \Pi^A_{\rho_f}$，因为$a_i \in [a_i]_{\rho_f}$，所以$\varphi(a_i)=[a_i]_{\rho_f}$，因此$\varphi$是满射.

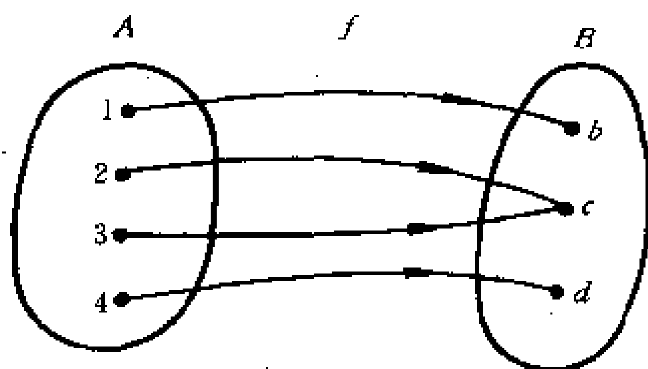
又对于任意$a \in A$，有

$$g \cdot \varphi(a) = g(\varphi(a)) = g([a]_{\rho_f}) = f(a),$$

于是由a的任意性，$g \cdot \varphi = f$.

下面通过一简单的例子来说明例A-11的结论.

例A-12 设$A=\{1,2,3,4\}$，$B=\{b,c,d\}$. 定义一由A到B的满射函数f，如图A-3所示.



图A-3

于是$\Pi^A_{\rho_f}=\{[1]_{\rho_f},[2]_{\rho_f},[4]_{\rho_f}\}=\{\{1\},\{2,3\},\{4\}\}$.

定义由$\Pi^A_{\rho_f}$到B的双射函数g如图A-4所示. 因为$[2]_{\rho_f}=[3]_{\rho_f}$，所以集合$\Pi^A_{\rho_f}$中的元素$[2]_{\rho_f}$也可以表示为$[3]_{\rho_f}$.

定义由A到$\Pi^A_{\rho_f}$的满射φ如图A-5所示.

根据函数f，g和φ的定义，我们很容易看出$f=g \cdot \varphi$

例A-13 设91函数$f: Z \to Z$（这里Z表示非负整数集）定义为

$$\begin{cases} f(n) = n - 10, & 若 n > 100; \\ f(n) = f(f(n+11)), & 若 n \leqslant 100, \end{cases}$$

试证明 a) $f(100)=91$；b) $f(n)=91 \quad (0 \leqslant n \leqslant 100)$，

证 a) $f(100)=f(f(100+11))=f(f(111))$

$$=f(111-10)=f(101)$$

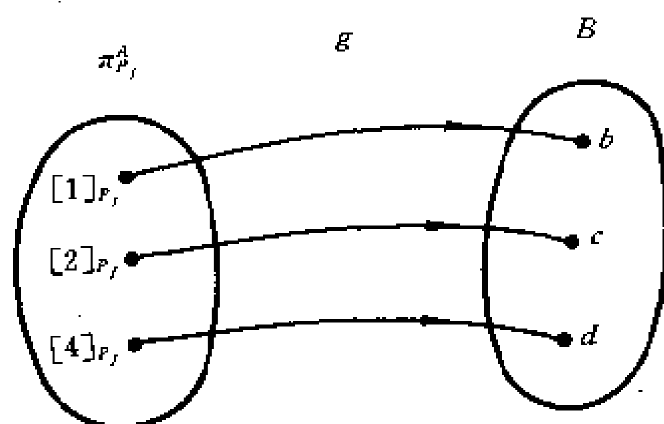


图 A-4

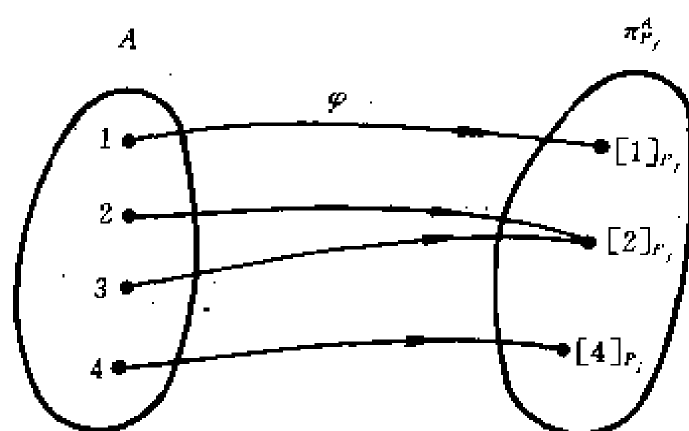


图 A-5

$=101-10=91.$

b)证明分为两部分：

(1) 证明对于所有的 $90\leqslant n\leqslant 100, f(n)=91$.

当 $n=100$ 时，由 a) 得 $f(100)=91$.

假设当 $n=k$ 时，$f(k)=91(91\leqslant k\leqslant 100)$，则对于 $90\leqslant k-1\leqslant 99$，

$$f(k-1)=f(f(k-1-11))=f(f(k+10)),$$

因为 $101\leqslant k+10\leqslant 110$，所以

$$f(k-1)=f(f(k+10))=f(k+10-10)=f(k)=91.$$

由上证得对于所有的 $90\leqslant n\leqslant 100, f(n)=91$.

(2) 证明当 $n<90$ 时，$f(n)=91$

设 $n<90$，且设 k 为使得 $90\leqslant n+11k\leqslant 100$ 的最小正整数，则

$$\begin{aligned} f(n) &= f(f(n+11)) = f(f(f(n+2\cdot 11))) \\ &= \cdots = f^k(f(n+k\cdot 11)) = f^k(91). \end{aligned}$$

由(1) 知 $f(91)=91$，因此对于任意 $k\geqslant 1$，$f^k(91)=91$. 于是对于 $n<90$，有 $f(n)=91$.

第二部分　代数系统

第四章　代数系统

4.1　内容提要

1. 集合 A 上的运算

- 集合 A 上的运算；
- 运算的封闭性；
- 二元运算的一些常见的性质；
- 集合中与二元运算相联系的一些特殊的元素：单位元、零元、幂等元、元素的逆元.

2. 代数系统

- 代数系统；
- 整环及其性质；
- 子代数

3. 代数系统的同态与同构

- 同态
- 满同态
- 满同态的性质
- 同构

4. 同余关系

- 同余关系

5. 积代数

4.2 基本知识点

1. 集合 A 上的运算

我们将笛卡尔积 A^n 到 A 的函数 $O:A^n \to A$ 称为集合 A 上的一个 n 元运算，因为对应关系 $O(a_1,a_2,\cdots,a_n)=a$ 可以看作是 A 中 n 个元素 $a_1,a_2,\cdots,a_n$ 经过某种运算后得到运算结果 a.

这里定义的运算与通常所说的运算重要区别在于：这里定义的运算与一个集合 A 紧密联系在一起，它要求运算对象和运算结果必须都是集合 A 中的元素. 由函数 $O:A^n \to A$ 的定义可知，A 中任意 n 个元素都可以进行这种运算，且运算结果是唯一的.

特别地，当 $n=2$ 或 $n=1$ 时，函数 $*:A^2 \to A$ 称作是集合 A 上的二元运算；函数 $\sim:A \to A$ 称为集合 A 上的一元运算. 对于任意的有序二元组 $(a_i,a_j)\in A^2$，我们常习惯地将 $*(a_i,a_j)=a$ 写作 $a_i * a_j=a$.

例 4-1 通常数的乘法运算是否可看作下列集合上的二元运算？请逐个回答，并说明理由.

(1) $A=\{1,2\}$；

(2) $B=\{x|x$ 是素数$\}$；

(3) $C=\{x|x$ 是偶数$\}$；

(4) $D=\{2^n|n\in N\}$.

解 (1) 乘法运算不是集合 A 上的二元运算. 因为 $2\times 2=4\notin A$.

(2) 乘法运算不是集合 B 上的二元运算. 因为素数乘素数不

再是素数. 例如 $3\times5=15\notin B$.

(3) 乘法运算是集合 C 上的运算. 因为偶数乘偶数仍为偶数.

(4) 乘法运算是集合 D 上的二元运算. 因为对于任意 2^n, $2^m\in D$, $2^n\times2^m=2^{n+m}\in D$.

例 4-2 设有集合 A, $A^A=\{f\mid f:A\to A\}$ 是由 A 到 A 的所有函数组成的集合. 因为对于任意 $f_1,f_2\in A^A$, f_1 与 f_2 的复合函数 $f_1\cdot f_2$ 仍是一由 A 到 A 的函数, 因此函数的复合运算可看作是集合 A^A 上的一个二元运算.

2. 运算的封闭性

若运算 o 是定义在集合 A 上的一个 n 元运算, 那么根据函数 $o:A^n\to A$ 的定义, 对于任意 $a_1,a_2,\cdots,a_n\in A$, 恒有 $o(a_1,a_2,\cdots,a_n)\in A$. 即当运算对象取自 A 时, 运算结果也仍在 A 中, 我们将运算的这一性质称作 o 在 A 上是封闭的.

设 o 是集合 A 上的一个 n 元运算, S 是 A 的一个非空子集, 若对于任意 $a_1,a_2,\cdots,a_n\in S$, 恒有 $o(a_1,a_2,\cdots,a_n)\in S$, 则称 o 在 A 的子集 S 上是封闭的.

对于 A 的任一非空子集 S, 集合 A 上的运算 o 在 S 上不一定是封闭的.

例 4-3 通常数的加法运算可看作是正整数集 N 上的一个二元运算. 下列集合均是 N 的子集, 加法运算在这些子集上是封闭的吗? 说明理由.

(1) $S_1=\{n\mid n$ 是 15 的因子$\}$;

(2) $S_2=\{n\mid n$ 是 15 的倍数$\}$;

(3) $S_3=\{n\mid 6$ 整除 n, 而 24 整除 $n^2\}$.

解 (1) 加法运算在 S_1 上不封闭. 因为 $3\in S_1$, $5\in S_1$, 但 $3+5=8\notin S_1$.

(2) 加法运算在 S_2 上是封闭的. 其证明如下:

对于任意 $n_1,n_2\in S_2$, 设 $n_1=15k_1$, $n_2=15k_2$ $(k_1,k_2\in N)$, 则

$n_1+n_2=15k_1+15k_2=15(k_1+k_2)$,$(k_1+k_2\in N)$. 因此 $n_1+n_2\in S_2$.

(3) 加法运算在 S_3 上是封闭的. 其证明如下:

首先,对于任意 $n_1,n_2\in S_3$,设 $n_1=6k_1,n_2=6k_2(k_1,k_2\in N)$,则 $n_1+n_2=6k_1+6k_2=6(k_1+k_2)$,$n_1+n_2$ 能被 6 整除.

又 $(n_1+n_2)^2=n_1^2+2n_1\cdot n_2+n_2^2$,根据题意,$n_1^2$ 能被 24 整除,n_2^2 能被 24 整除,而

$$2n_1\cdot n_2=2\cdot 6k_1\cdot 6k_2=24\cdot(3k_1k_2)$$

也能被 24 整除,因此 $(n_1+n_2)^2$ 能被 24 整除. 由此知 $n_1+n_2\in S_3$.

例 4-4 设 W 是集合 A 上所有关系的集合,H_1 是 A 上所有自反关系的集合,H_2 是 A 上所有可传递关系的集合. 显然关系的复合运算是 W 上的一个二元运算,试问关系的复合运算在 H_1 和 H_2 上是封闭的吗?为什么?

解 关系的复合运算 $\circ$ 在 H_1 上是封闭的. 因为 A 上任意两个自反关系的复合关系仍是 A 上的自反关系. 但 $\circ$ 在 H_2 上不封闭. 因为 A 上任意两个可传递关系的复合关系不一定是可传递的. 例如

设 $A=\{1,2,3\}$,定义集合 A 上的关系

$$\rho_1=\{(1,2),(2,3),(1,3)\};$$

$$\rho_2=\{(2,3),(3,1),(2,1)\}.$$

显然 ρ_1 和 ρ_2 均是可传递的.

$$\rho_1\cdot\rho_2=\{(1,3),(1,1),(2,1)\}.$$

但 $\rho_1\cdot\rho_2$ 不可传递.

3. 二元运算的一些常见的性质

集合 A 上的二元运算与通常数的加法、乘法运算一样,也可以具有某些性质,如交换律、结合律和分配律等.

例 4-5 实数集 R 上的下列二元运算是否满足交换律和结合律?

(1) $r_1*r_2=r_1+r_2-r_1r_2$;

(2) $r_1 \circ r_2 = \frac{1}{2}(r_1 + r_2)$.

解 (1) 因为 $r_1 * r_2 = r_1 + r_2 - r_1 r_2 = r_2 + r_1 - r_2 r_1 = r_2 * r_1$，所以运算 * 满足交换律. 又

$$
\begin{aligned}
(r_1 * r_2) * r_3 &= (r_1 + r_2 - r_1 r_2) * r_3 \\
&= (r_1 + r_2 - r_1 r_2) + r_3 - (r_1 + r_2 - r_1 r_2) r_3 \\
&= r_1 + r_2 + r_3 - r_1 r_2 - r_1 r_3 - r_2 r_3 + r_1 r_2 r_3, \\
r_1 * (r_2 * r_3) & \\
&= (r_2 * r_3) * r_1 = (r_2 + r_3 - r_2 r_3) * r_1 \\
&= r_2 + r_3 - r_2 r_3 + r_1 - (r_2 + r_3 - r_2 r_3) r_1 \\
&= r_1 + r_2 + r_3 - r_2 r_3 - r_1 r_2 - r_1 r_3 + r_1 r_2 r_3,
\end{aligned}
$$

所以 $(r_1 * r_2) * r_3 = r_1 * (r_2 * r_3)$，因此运算 * 满足结合律.

(2) 因为 $r_1 \circ r_2 = \frac{1}{2}(r_1 + r_2) = \frac{1}{2}(r_2 + r_1) = r_2 \circ r_1$

所以运算 $\circ$ 满足交换律. 又

$$
\begin{aligned}
r_1 \circ (r_2 \circ r_3) &= r_1 \circ \frac{1}{2}(r_2 + r_3) = \frac{1}{2}(r_1 + \frac{1}{2}(r_1 + r_3)) \\
&= \frac{r_1}{2} + \frac{r_2}{4} + \frac{r_3}{4}; \\
(r_1 \circ r_2) \circ r_3 &= \frac{1}{2}(r_1 + r_2) \circ r_3 = \frac{1}{2}(\frac{1}{2}(r_1 + r_2) + r_3) \\
&= \frac{r_1}{4} + \frac{r_2}{4} + \frac{r_3}{2}.
\end{aligned}
$$

一般情形下 $\frac{r_1}{2} + \frac{r_2}{4} + \frac{r_3}{4} \neq \frac{r_1}{4} + \frac{r_2}{4} + \frac{r_3}{2}$，因此运算 $\circ$ 不满足结合律.

4. 集合中与二元运算相联系的一些特殊元素

设 * 是集合 A 上的二元运算.

(1) 单位元：若存在元素 $e \in A$，使得对于任意的 $a \in A$，有 $e * a = a * e = a$，则称 e 是 A 中关于运算 * 的单位元.

(2) 零元：若存在元素 $z \in A$，使得对于任意的 $a \in A$，有 $a * z$

$=z*a=z$,则称 z 是 A 中关于运算 $*$ 的零元.

(3) 幂等元:若元素 $a\in A$,满足 $a*a=a$,则称 a 是 A 中关于运算 $*$ 的幂等元.

(4) 元素的逆元:对于某元素 $a\in A$,若相应存在一元素 $b\in A$,使得 $a*b=b*a=e$(e 是单位元),则称元素 a 关于运算 $*$ 是可逆的. 称 b 是 a 的逆元. a 的逆元常记作 a^{-1}.

例4-6 例 4-5 中运算 $*$ 是否存在单位元、零元和幂等元?若有单位元的话,哪些元素有逆元?

解 运算 $*$ 的定义是 $r_1*r_2=r_1+r_2-r_1r_2$.

(1) 若 r_1 是单位元,则对于任意的 $r\in R$,有

$$r_1*r=r*r_1=r,$$

由于 $*$ 是可交换的,仅考虑 $r_1*r=r$,即

$$r_1+r-r_1r=r,$$

于是 $$r_1-r_1r=0,\quad r_1(1-r)=0.$$

由于 r 是任意的,要使上式成立,只有 $r_1=0$,因此 0 是运算 $*$ 的单位元.

(2) 若 r_1 是零元,则对于任意的 $r\in R$,应有

$$r_1*r=r*r_1=r_1,$$

仅考虑 $r_1*r=r_1$,即

$$r_1+r-r_1r=r_1$$

于是

$$r-r_1r=0,\quad r(1-r_1)=0.$$

由于 r 是任意的,要使上式成立,只有 $r_1=1$,因此 1 是运算 $*$ 的零元.

(3) 若 $r\in R$ 是幂等元,则应有 $r*r=r$,即

$$r+r-r^2=r,$$

于是 $$r-r^2=0,\quad r(1-r)=0$$

要使上式成立,只有 $r=0$ 或 $r=1$,因此 0 和 1 是幂等元.

(4) 设 r_2 是 r_1 的逆元,则应有

$$r_1 * r_2 = r_1 + r_2 - r_1 r_2 = 0,$$

于是

$$r_2(r_1 - 1) = r_1, \quad r_2 = \frac{r_1}{r_1 - 1}$$

因此，只要 $r \neq 1$，R 中任意元素 r 均有逆元，其逆元是$\frac{r}{r-1}$.

由单位元和零元的唯一性可知，R 中除 0 和 1 以外，没有其它任何的单位元和零元. 由运算的可结合性知，任意元素 $r(r \neq 1)$ 的逆元也是唯一的.

例 4-7 实数集 R 上的二元运算 $*$ 定义为

$$r_1 * r_2 = r_1 + \frac{1}{2} r_2$$

集合 R 中关于运算 $*$ 存在有单位元、零元和幂等元吗?

解 (1) 运算 $*$ 不可交换，因此我们分别考虑它是否有左单位元和右单位元.

若 r_1 是左单位元，则对于任意 $r \in R$，应有

$$r_1 * r = r, \quad r_1 + \frac{r}{2} = r,$$

于是 $r_1 = \frac{r}{2}$.

由于 r 是任意的，因此不存在元素能成为运算 $*$ 的左单位元. 由此可知 $*$ 不存在单位元.

若 r_1 是右单位元，则对于任意 $r \in R$，应有

$$r * r_1 = r, \quad r + \frac{r_1}{2} = r$$

要使上式成立，只有 $r_1 = 0$，因此 0 是运算 $*$ 的右单位元.

(2) 若 r_1 是左零元，则对于任意的 $r \in R$，应有

$$r_1 * r = r_1, \quad r_1 + \frac{r}{2} = r_1$$

要使上式成立，必须 $r = 0$，但 r 是任意的，因此运算 $*$ 没有左零元. 由此可知运算 $*$ 不存在零元.

若 r_1 是右零元，则对于任意的 $r\in R$，应有

$$r*r_1=r_1,\quad r+\frac{r_1}{2}=r_1,$$

于是

$$r=\frac{r_1}{2},\quad r_1=2r$$

由于 r 是任意的，因此运算 $*$ 也没有右零元.

(3) 若 $r\in R$ 是幂等元，则应有

$$r+\frac{r}{2}=r,\quad \frac{r}{2}=0.$$

要使上式成立，必须 $r=0$，因此 0 是幂等元.

5. 代数系统

定义在非空集合 S 上的一个或若干个运算和 S 一起组成一个代数系统，记作 $\langle S;o_1,o_2,\cdots,o_n\rangle$，其中 $o_1,o_2,\cdots,o_n$ 表示定义在 S 上的 n 个运算.

例 4-8 设有集合 A、B，并设 $W=\{\rho|\rho$ 是由 A 到 B 的关系$\}$. 因为由 A 到 B 的任一关系均是 $A\times B$ 的一个子集，所以任意两个关系经过并运算和交运算后，其结果仍是 $A\times B$ 的一个子集，即仍是由 A 到 B 的一个关系. 若将 $A\times B$ 看作是全集合，则关系 ρ 的补 ρ' 也是 $A\times B$ 的一个子集，即也是由 A 到 B 的一个关系. 因此集合的并运算、交运算和补运算可分别看作是 W 上的二元运算和一元运算. 于是 $\langle W;\cup,\cap,'\rangle$ 是一代数系统.

例如 设 $A=\{0,1\}$，$B=\{a,b,c\}$，

则 $\quad A\times B=\{(0,a),(0,b),(0,c),(1,a),(1,b),(1,c)\}$.

设 A 到 B 的关系

$$\rho_1=\{(0,a),(0,c),(1,a)\};$$

$$\rho_2=\{(0,b),(0,c),(1,c)\};$$

则 $\quad \rho_1\cup\rho_2=\{(0,a),(0,b),(0,c),(1,a),(1,c)\};$

$$\rho_1\cap\rho_2=\{(0,c)\};$$

$$\rho_1' = \{(0,b),(1,b),(1,c)\}.$$

也都是由 A 到 B 的关系.

6. 整环及其性质

整环$\langle J;+,\cdot\rangle$是一类代数系统的总称,因此它是一种抽象的代数系统.在非空集合 J 上定义的这两个二元运算必须满足以下六个条件:

(1) $+$和$\cdot$都是可交换的;

(2) $+$和$\cdot$都是可结合的;

(3) $\cdot$对$+$是可分配的;

(4) $+$和$\cdot$均有单位元(将$+$的单位元记作 0,将$\cdot$的单位元记作 1);

(5) 每一元素 $x\in J$ 在 J 中均有加法逆元$-x$,使得 $x+(-x)=(-x)+x=0$;

(6) $\cdot$满足消去律.

凡在一个非空集合上定义了两个二元运算,且这两个运算满足上述六条性质的代数系统,均称为整环.

例 4-9 设 $A=\left\{\begin{bmatrix} a & b \\ 2b & a \end{bmatrix} \middle| a,b\in I\right\}$,试证明集合 A 与矩阵的加法和乘法运算构成一个整环(这里 I 表示整数集).

证 对于任意的$\begin{bmatrix} a & b \\ 2b & a \end{bmatrix}$、$\begin{bmatrix} c & d \\ 2d & c \end{bmatrix}\in A$;

因为

$$\begin{bmatrix} a & b \\ 2b & a \end{bmatrix}+\begin{bmatrix} c & d \\ 2d & c \end{bmatrix}=\begin{bmatrix} a+c & b+d \\ 2(b+d) & a+c \end{bmatrix}\in A;$$

$$\begin{bmatrix} a & b \\ 2b & a \end{bmatrix}\cdot\begin{bmatrix} c & d \\ 2d & c \end{bmatrix}=\begin{bmatrix} ac+2bd & ad+bc \\ 2(bc+ad) & 2bd+ac \end{bmatrix}\in A,$$

所以$\langle A;+,\cdot\rangle$构成一个代数系统.

(1) 根据矩阵加法运算的定义,$+$满足交换律.对于运算$\cdot$,

因为

$$\begin{bmatrix} c & d \\ 2d & c \end{bmatrix} \cdot \begin{bmatrix} a & b \\ 2b & a \end{bmatrix} = \begin{bmatrix} ac+2bd & bc+ad \\ 2(ad+bc) & 2bd+ac \end{bmatrix}$$

与前面计算的$\begin{bmatrix} a & b \\ 2b & a \end{bmatrix} \cdot \begin{bmatrix} c & d \\ 2d & c \end{bmatrix}$相等，所以 · 也满足交换律.

(2) 矩阵的加法和乘法运算均满足结合律.

(3) 矩阵的乘法运算对加法运算是可分配的.

(4) 矩阵$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$是加法运算的单位元.

矩阵$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$是乘法运算的单位元.

(5) 对任意$\begin{bmatrix} a & b \\ 2b & a \end{bmatrix} \in A$，其加法逆元是矩阵$\begin{bmatrix} -a & -b \\ -2b & -a \end{bmatrix}$.

(6) 所谓运算 · 满足消去律是指，对于任意的矩阵 x、y、$z \in A$，若 $x \neq 0$，则由 $x \cdot y = x \cdot z$，可得 $y = z$. 这里 $x \neq 0$ 指 x 不是加法运算的单位元.

设$\begin{bmatrix} a & b \\ 2b & a \end{bmatrix}$、$\begin{bmatrix} c & d \\ 2d & c \end{bmatrix}$、$\begin{bmatrix} e & f \\ 2f & e \end{bmatrix} \in A$，其中 a,b 至少有一个不为 0. 并设

$$\begin{bmatrix} a & b \\ 2b & a \end{bmatrix} \cdot \begin{bmatrix} c & d \\ 2d & c \end{bmatrix} = \begin{bmatrix} a & b \\ 2b & a \end{bmatrix} \cdot \begin{bmatrix} e & f \\ 2f & e \end{bmatrix},$$

于是

$$\begin{bmatrix} ac+2bd & ad+bc \\ 2(bc+ad) & 2bd+ac \end{bmatrix} = \begin{bmatrix} ae+2bf & af+be \\ 2(be+af) & 2bf+ac \end{bmatrix},$$

因此

$$ac+2bd = ae+2bf, \tag{1}$$

$$ad+bc = af+be. \tag{2}$$

将(1)式两边同乘以 a，将(2)式两边同乘以 $2b$，分别得

$$a^2c+2abd = a^2e+2abf, \tag{3}$$

$$2abd+2b^2c = 2abf+2b^2e, \tag{4}$$

(3)－(4)得

$$(a^2-2b^2)c=(a^2-2b^2)e,$$

$$(a^2-2b^2)(c-e)=0,$$

因此 $a^2-2b^2=0$ 或 $c-e=0$.

因为 a、b 均为整数，且 a、b 中至少一个不为 0，所以 $a^2-2b^2\neq 0$，因此必有 $c=e$.

类似地可以证明 $d=f$，故

$$\begin{bmatrix} c & d \\ 2d & c \end{bmatrix}=\begin{bmatrix} e & f \\ 2f & e \end{bmatrix}.$$

由上可知 $\langle A;+,\cdot\rangle$ 是一整环.

例 4-10 设 $\langle J;+,\cdot\rangle$ 是一整环. 试证明

(1) 对所有的 $i,j,k\in J$，若 $i+j=i+k$；则 $j=k$.

(2) 对所有的 $i\in J$，有 $i\cdot 0=0\cdot i=0$；

(3) 对所有的 $i\in J$，有 $-i=(-1)\cdot i$.

证 (1) 由 $i+j=i+k$，在等式两边同时加上 i 的加法逆元 $-i$，得

$$(-i)+i+j=(-i)+i+k$$

由加法的结合律得 $\qquad 0+j=0+k$

所以 $\qquad j=k$

(2) 因为 $i\cdot 0+i\cdot 0=i\cdot(0+0)=i\cdot 0$，

所以 $\qquad i\cdot 0+i\cdot 0=i\cdot 0+0.$

由(1)得 $\qquad i\cdot 0=0,$

由交换性得 $\qquad i\cdot 0=0\cdot i=0.$

(3) 对任意的 $i\in J$，

$$\begin{aligned}(-1)\cdot i+i &=(-1)\cdot i+1\cdot i && (1\text{ 是运算}\cdot\text{的单位元})\\ &=((-1)+1)\cdot i && (\cdot\text{ 对}+\text{可分配})\\ &=0\cdot i && (-1\text{ 是 }1\text{ 的加法逆元})\\ &=0 && (\text{由}(2))\end{aligned}$$

又由运算 + 的交换性，$(-1)\cdot i+i=i+(-1)\cdot i=0$，因此 $(-1)\cdot i$ 是 i 的加法逆元，故 $(-1)\cdot i=-i$.

除了上述三条性质外，还可以列出整环的其它一些性质；这些性质对于任何一个满足整环定义的代数系统均是成立的.

7. 子代数

设$\langle S;o_1,o_2,\sim\rangle$是一代数系统，其中$o_1$、$o_2$是二元运算，$\sim$是一元运算. 若$H$是$S$的一个非空子集，且$S$上的运算$o_1$、$o_2$和$\sim$在$H$上都是封闭的，那么若将这几个运算的定义域分别由$S^2$缩小为$H^2$，将值域包由$S$缩小为$H$，则这几个运算也分别可看作是$H$上的二元运算和一元运算. 因此也构成代数系统$\langle H;o_1,o_2,\sim\rangle$. 我们称它为$\langle S;o_1,o_2,\sim\rangle$的子代数.

例 4-11 设$V=\langle I;+,\cdot\rangle$，其中$I$表示整数集，$+$和$\cdot$分别表示通常数的加法和乘法运算. 对下面$I$的每个子集，确定它是否能构成$V$的子代数？为什么？

(1) $H_1=\{2n+1|n\in I\}$；

(2) $H_2=\{-1,0,1\}$；

(3) $H_3=\{2n|n\in I\}$.

解 (1) H_1不能构成V的子代数.

因为对于任意的$2n_1+1,2n_2+1\in H_1$，有

$$(2n_1+1)+(2n_2+1)=2n_1+2n_2+2\notin H_1$$

所以加法运算在H_1上不封闭.

(2) H_2也不能构成V的子代数.

因为加法运算在H_2上也不封闭. 例如，$1+1=2\notin H_2$.

(3) H_3能构成V的子代数.

因为对于任意的$2n_1,2n_2\in H_3$，有$2n_1+2n_2=2(n_1+n_2)\in H_3$，$2n_1\cdot 2n_2=2(2n_1n_2)\in H_3$，所以加法运算和乘法运算在$H_3$上均是封闭的. 因此$\langle H_3;+,\cdot\rangle$是$\langle I;+,\cdot\rangle$的子代数.

在代数系统$V=\langle I;+,\cdot\rangle$中，将运算$+$去掉，令$V_1=\langle I;\cdot\rangle$. 由于运算$\cdot$在$H_1$和$H_2$上是封闭的，因此$\langle H_1;\cdot\rangle$和$\langle H_2;\cdot\rangle$均可看作是$V_1$的子代数.

例 4-12 设$V=\langle R;*\rangle$，其中R是实数集，运算$*$定义为

$$x*y=[x,y].$$

符号$[x,y]$表示不小于x和y的最小整数，又设

$$H_1=\{x|0\leqslant x\leqslant 10,x\in R\};$$

$$H_2=\{x|0\leqslant x<10,x\in R\},$$

试问H_1与H_2能否构成V的子代数？

解 正确理解符号$\lceil x,y\rceil$的含义．例如

$$\lceil 1.5,\sqrt{2}\rceil=2,\lceil -3,-2.1\rceil=-2.$$

因为运算$*$在H_1上是封闭的，所以$\langle H_1;*\rangle$是$\langle R;*\rangle$的子代数．但H_2与运算$*$不能构成V的子代数，因为$*$在H_2上不封闭．例如$\lceil 9.8,2\rceil=10$，但$10\notin H_2$．

8. 代数系统的同态

设有两个代数系统$V_1=\langle S_1;o_1,*_1,\sim_1\rangle$和$V_2=\langle S_2;o_2,*_2,\sim_2\rangle$，其中运算$o_i$和$*_i(i=1,2)$都是二元运算，$\sim_i(i=1,2)$是一元运算．所谓$h$是从$V_1$到$V_2$的一个同态是指$h$是一个从$S_1$到$S_2$的函数，并且$h$对于这些运算应满足以下的条件：对于任意的$\langle x_1,x_2\rangle\in S_1^2$，有

$$h(x_1o_1x_2)=h(x_1)o_2h(x_2);$$

$$h(x_1*_1x_2)=h(x_1)*_2h(x_2).$$

对于任意的$x\in S_1$，有

$$h(\sim_1(x))=\sim_2(h(x)).$$

例 4-13 设有代数系统$V_1=\langle R;+,\sim\rangle$和$V_2=\langle R_+;\cdot,'\rangle$，其中$R$和$R_+$分别表示实数集和正实数集，$+$和$\cdot$是通常数的加法和乘法，$\sim$表示求相反数的运算，$'$表示求倒数的运算．

设有函数$h:R\to R_+$，对于任意$x\in R$，$h(x)=e^x$．于是对于任意$x,y\in R$，

$$h(x+y)=e^{x+y}=e^x\cdot e^y=h(x)\cdot h(y).$$

对于任意 $x\in R$,

$$h(\sim(x))=h(-x)=e^{-x}=\frac{1}{e^x}=(h(x))'.$$

因此 h 是由 V_1 到 V_2 的一个同态.

9. 满同态

若 h 是从代数系统 V_1 到 V_2 的同态,且 h 又是一个满射,则称 h 是从 V_1 到 V_2 的满同态.满同态 h 可以将 V_1 中运算的性质保持到 V_2 中的运算.也就是说 V_1 中运算若具有某些性质,诸如交换律、结合律、分配律、单位元、零元、元素有逆元等,只要由 V_1 到 V_2 存在着满同态,则 V_2 中相应的运算也具有上述这些性质.

例 4-14 设 $V=\langle R^*;\cdot\rangle$,其中 R^* 表示非零实数集,$\cdot$ 表示通常数的乘法运算.试问下列两个函数是否由 V 到 V 的满同态?

(1) $h(x)=x^2$;

(2) $g(x)=\frac{1}{x}$.

解 (1) 对任意 $x\in R^*$,有 $x^2\in R^*$,所以 h 是由 R^* 到 R^* 的函数.又对于任意 $x,y\in R^*$,有

$$h(x\cdot y)=(x\cdot y)^2=x^2\cdot y^2=h(x)\cdot h(y),$$

所以 h 是从 V 到 V 的同态.

但 h 不是从 V 到 V 的满同态.因为 h 不是由 R^* 到 R^* 的满射,例如 $-5\in R^*$,但不存在 $x\in R^*$,使 $x^2=-5$.

(2) 对任意 $x\in R^*$,因为 $x\neq0$,所以有 $\frac{1}{x}\in R^*$,因此 g 是由 R^* 到 R^* 的函数.又对于任意 $x,y\in R^*$,

有 $$g(x\cdot y)=\frac{1}{x\cdot y}=\frac{1}{x}\cdot\frac{1}{y}=g(x)\cdot g(y),$$

所以 g 是从 V 到 V 的同态.

对于任意 $x\in R^*$,有 $\frac{1}{x}\in R^*$,且 $\frac{1}{\frac{1}{x}}=x$,因此 $g(\frac{1}{x})=x$.即 R^* 中任一元素在 R^* 中均有像源.所以 g 是由 R^* 到 R^* 的满射,因此

g 是从 V 到 V 的满同态.

10. 同构

若 h 是从代数系统 V_1 到 V_2 的同态，而 h 又是一双射，则称 h 是从 V_1 到 V_2 的同构. 同构也是满同态，因此它也能"保持运算的性质".

我们知道，若 h 是从 V_1 到 V_2 的同构，则它的逆函数 h^{-1} 必是从 V_2 到 V_1 的同构，因此代数系统的同构关系是一对称关系.

例 4-15 设 $A=\{a,b,c\}$，试问代数系统 $\langle\{\varnothing,A\};\cup,\cap\rangle$ 和 $\langle\{\{a,b\},A\};\cup,\cap\rangle$ 是否同构？

解 令 $S=\{\varnothing,A\}$，$H=\{\{a,b\},A\}$. 定义函数 $f:S\to H$，使得 $f(\varnothing)=\{a,b\}$，$f(A)=A$. 显然 f 是一双射.

对于任意 $x,y\in S$，若 $x=y$，则

$$f(x\cup y)=f(x),$$

$$f(x)\cup f(y)=f(x)\cup f(x)=f(x),$$

所以有 $$f(x\cup y)=f(x)\cup f(y).$$

若 $x\neq y$，则

$$f(x\cup y)=f(A)=A,$$

$$f(x)\cup f(y)=\{a,b\}\cup A=A.$$

所以有 $$f(x\cup y)=f(x)\cup f(y).$$

因此对于任意 $x,y\in S$，都有 $f(x\cup y)=f(x)\cup f(y)$.

类似地对于任意 $x,y\in S$，若 $x=y$，则

$$f(x\cap y)=f(x);$$

$$f(x)\cap f(y)=f(x)\cap f(x)=f(x);$$

所以有 $$f(x\cap y)=f(x)\cap f(y).$$

若 $x\neq y$，则

$$f(x\cap y)=f(\varnothing)=\{a,b\};$$

$$f(x)\cap f(y)=\{a,b\}\cap A=\{a,b\},$$

所以有 $$f(x\cap y)=f(x)\cap f(y).$$

因此对于任意的 $x,y\in S$，都有 $f(x\cap y)=f(x)\cap f(y)$.

由上证得 $\langle\{\varnothing,A\};\cup,\cap\rangle$ 与 $\langle\{\{a,b\},A\},\cup,\cap\rangle$ 同构.

例 4-16 代数系统 $V_1=\langle I;+\rangle$ 与 $V_2=\langle N;\cdot\rangle$ 是否同构？这里 I 和 N 分别表示整数集和正整数集，$+$ 和 $\cdot$ 分别表示通常数的加法和乘法.

解 I 和 N 都是可数集，因此 I 和 N 之间存在有双射. 例如可以定义函数 $f:I\to N$，使得

$$f(i)=\begin{cases}1, & 若\ i=0;\\ 2i, & 若\ i>0;\\ 2|i|+1, & 若\ i<0.\end{cases}$$

因为 I 和 N 均是无限集，因此由 I 到 N 可以定义许多甚至无穷多个双射函数. 这些双射函数中是否有满足同态条件的呢？我们不可能对所有的双射函数去一一考察，为了回答这一问题，我们可以先来考察这两个代数系统所具有的性质.

$\langle I;+\rangle$ 中运算 $+$ 具有单位元 0；$\langle N;\cdot\rangle$ 中运算 $\cdot$ 也具有单位元 1.

$\langle I;+\rangle$ 中每一整数 i 对于运算 $+$ 均有逆元 $-i$，即 $i+(-i)=(-i)+i=0$；但 $\langle N;\cdot\rangle$ 中除单位元 1 对于运算 $\cdot$ 具有逆元 1 外，其它正整数对于运算 $\cdot$ 均不存在逆元. 这就是说，任何一个由 I 到 N 的双射函数都不能使 V_2 中运算 $\cdot$ 具有 V_1 中运算 $+$ 每一元素均有逆元的这一条性质. 而"保持运算的性质"是 f 为同构的必要条件，由此可知 V_1 与 V_2 不同构.

11. 对于运算的代换性质

设代数系统 $V=\langle S;\circ,\sim\rangle$，其中，$\circ$ 是二元运算，$\sim$ 是一元运算. ρ 是 S 上的一个等价关系，若对于任意的 $x,y\in S$.

由 $x\rho y$，可得 $(\sim x)\rho(\sim y)$，

则称 ρ 对于运算 $\sim$ 满足代换性质.

对于任意的 $x_1,x_2,y_1,y_2\in S$，若由 $x_1\rho y_1$，$x_2\rho y_2$，可得 $(x_1\circ x_2)$

$\rho(y_1 \circ y_2)$，则称 ρ 对于运算 $\circ$ 满足代换性质.

例 4-17 设代数系统 $V=\langle I;+,\sim\rangle$，其中 I 和 $+$ 的含义同例 4-16，$\sim$ 表示求相反数的运算. 定义 I 上的二元关系 ρ：对于任意 $x,y\in I$，当且仅当 $x<0,y<0$ 或者 $x\geqslant 0,y\geqslant 0$ 时，$x\rho y$. 试问 ρ 是否 I 上的等价关系？若是等价关系，ρ 对运算 $+$ 和 $\sim$ 是否满足代换性质？

解 对于任意 $x\in I$，或者有 $x<0$，或者有 $x\geqslant 0$，所以总有 $x\rho x$.

对于任意 $x,y\in I$，若 $x\rho y$，则或者 $x<0,y<0$，或者 $x\geqslant 0,y\geqslant 0$，即 $y<0,x<0$ 或者 $y\geqslant 0,x\geqslant 0$，因此有 $y\rho x$.

对于任意 $x,y,z\in I$，若 $x\rho y,y\rho z$，则由 $x\rho y$，有 $x<0,y<0$ 或者 $x\geqslant 0,y\geqslant 0$.

若 $x<0,y<0$，则由 $y\rho z$，必有 $z<0$，因此 $x\rho z$.

若 $x\geqslant 0,y\geqslant 0$，则由 $y\rho z$，必有 $z\geqslant 0$，因此 $x\rho z$.

由上可知，ρ 是 I 上的等价关系.

ρ 对于运算 $+$ 不满足代换性质. 例如，$-2\rho-8$，$5\rho 5$，$(-2)+5=3$，$(-8)+5=-3$，但 $3\rho-3$ 不成立.

ρ 对于运算 $\sim$ 也不满足代换性质. 例如，$0\rho 5$，$\sim 0=0$，$\sim 5=-5$，但 $0\rho-5$ 不成立.

例 4-18 代数系统 $V=\langle I;\cdot,\sim\rangle$，其中 I 和 $\sim$ 的含义同例 4-17，$\cdot$ 表示通常数的乘法运算. 定义 I 上的二元关系 ρ：对于任意 $x,y\in I$，当且仅当 $x=0,y=0$ 或者 $x\neq 0,y\neq 0$ 时，$x\rho y$. 试问 ρ 是否 I 上的等价关系？若是，ρ 对于运算 $\cdot$ 和 $\sim$ 是否满足代换性质？

解 类似于例 4-17，容易证明 ρ 是 I 上的等价关系.

ρ 对于运算 $\cdot$ 满足代换性质.

因为对于任意的 $x_1,y_1,x_2,y_2\in I$，若 $x_1\rho y_1,x_2\rho y_2$，则有 $x_1=0,y_1=0$ 或者 $x_1\neq 0,y_1\neq 0$.

若 $x_1=0,y_1=0$，则 $x_1\cdot x_2=0,y_1\cdot y_2=0$，因此有 $(x_1\cdot x_2)\rho(y_1\cdot y_2)$.

若 $x_1 \neq 0, y_1 \neq 0$，如果 $x_2 = 0, y_2 = 0$，显然 $(x_1 \cdot x_2)\rho(y_1 \cdot y_2)$；如果 $x_2 \neq 0, y_2 \neq 0$，则 $x_1 \cdot x_2 \neq 0, y_1 \cdot y_2 \neq 0$，因此 $(x_1 \cdot x_2)\rho(y_1 \cdot y_2)$.

ρ 对于运算～也满足代换性质.

因为对于任意 $x, y \in I$，若 $x\rho y$，则

$$x = 0, y = 0 \text{ 或者 } x \neq 0, y \neq 0,$$

于是
$$\sim x = 0, \sim y = 0 \text{ 或者} \sim x \neq 0, \sim y \neq 0,$$

因此总有 $(\sim x)\rho(\sim y)$.

12. 同余关系

设有代数系统 $V = \langle S; o_1, o_2, \cdots, o_n \rangle$，其中运算 $o_i (i = 1, 2, \cdots, n)$ 是 S 上的一元或二元运算，ρ 是 S 上的一个等价关系，若 ρ 对于 S 上的每一个运算均满足代换性质，则称 ρ 是 V 上的一个同余关系.

例如，例 4-17 中的等价关系 ρ 不是 $\langle I; +, \sim \rangle$ 上的同余关系，例 4-18 中的等价关系 ρ 是 $\langle I; \cdot, \sim \rangle$ 上的同余关系.

例 4-19 例 4-18 中的等价关系 ρ 是否是例 4-17 的代数系统 $V = \langle I; +, \sim \rangle$ 上的同余关系呢？

解 由例 4-18 知，ρ 对于运算～满足代换性质.

但对于运算 $+$，ρ 不满足代换性质. 例如，有 $-5\rho 3, 5\rho 4, (-5) + 5 = 0, 3 + 4 = 7$，但 $0\rho 7$ 不成立. 因此例 4-18 中的 ρ 不是 $\langle I; +, \sim \rangle$ 上的同余关系.

13. 商集与商代数

在第二章我们曾介绍过，若 ρ 是集合 A 上的等价关系，则等价类的集合 $\{[a]_\rho | a \in A\}$ 构成 A 的一个分划. 这一分划实际上是以 A 的一些非空子集为元素的集合，我们也将这一集合称为 A 关于等价关系 ρ 的商集，用 A/ρ 表示.

设有代数系统 $V = \langle S; o, \sim \rangle$，其中 o 和～分别是二元运算和

一元运算，ρ 是 V 上的同余关系. 令 $V^* = \langle S^*; o^*, \sim^* \rangle$，其中 $S^* = S/\rho = \{[x]_\rho | x \in S\}$，即 S^* 是 S 关于 ρ 的商集. 运算 o^* 和 $\sim^*$ 分别是 S^* 上的二元和一元运算，定义如下：

$$[x]_\rho o^* [y]_\rho = [xoy]_\rho,\ \sim^* [x]_\rho = [\sim (x)]_\rho,$$

则代数系统 V^* 称为是 V 关于 ρ 的商代数. 并表示为 V/ρ.

这一定义对于集合 S 上定义了任意多个运算的代数系统均是适用的.

例 4-20 代数系统 $V = \langle A; o_1, o_2 \rangle$，这里 $A = \{a_1, a_2, a_3, a_4, a_5\}$，运算 o_1 和 o_2 均是一元运算，由表 4-1 定义

表 4-1

a_i	$o_1(a_i)$	$o_2(a_i)$
a_1	a_4	a_3
a_2	a_3	a_2
a_3	a_4	a_1
a_4	a_2	a_3
a_5	a_1	a_5

A 上的等价关系 ρ 产生 A 的分划 $\{\{a_1, a_3\}, \{a_2, a_5\}, \{a_4\}\}$. 试证明 ρ 是 V 上的同余关系. 确定商代数 V/ρ（通过构造它的运算表）和从 V 到 V/ρ 的满同态.

证 因为 ρ 具有自反性，所以对于任意的 $a_i \in A$，由 $a_i \rho a_i$ 显然可得 $o_1(a_i) \rho o_1(a_i)$，$o_2(a_i) \rho o_2(a_i)$.

又因为 $o_1(a_1) = a_4$，$o_1(a_3) = a_4$，所以 $o_1(a_1) \rho o_1(a_3)$；

因为 $o_2(a_1) = a_3$，$o_2(a_3) = a_1$，所以 $o_2(a_1) \rho o_2(a_3)$；

因为 $o_1(a_2) = a_3$，$o_1(a_5) = a_1$，所以 $o_1(a_2) \rho o_1(a_5)$；

因为 $o_2(a_2) = a_2$，$o_2(a_5) = a_5$，所以 $o_2(a_2) \rho o_2(a_5)$.

由上可知 ρ 是 V 上的同余关系.

按照商代数的定义，商代数 $V/\rho = \{A/\rho; o_1^*, o_2^*\}$

其中 $$A/\rho = \{\{a_1, a_3\}, \{a_2, a_5\}, \{a_4\}\}.$$

运算 o_1^* 和 o_2^* 的定义由表 4-2 给出.

表 4-2

	o_1^*	o_2^*
$\{a_1,a_3\}$	$\{a_4\}$	$\{a_1,a_3\}$
$\{a_2,a_5\}$	$\{a_1,a_3\}$	$\{a_2,a_5\}$
$\{a_4\}$	$\{a_2,a_5\}$	$\{a_1,a_3\}$

定义函数 $f: A \to A/\rho$,对于任意 $a_i \in A$, $f(a_i)=[a_i]_\rho$. 即

$$f(a_1) = f(a_3) = \{a_1,a_3\};$$
$$f(a_2) = f(a_5) = \{a_2,a_5\};$$
$$f(a_4) = \{a_4\}.$$

显然 f 是一个满射. 又对于任意 $a_i \in A$ 和任意运算 $o_j(j=1, 2)$,

$$f(o_j(a_i)) = [o_j(a_i)]_\rho = o_j^*([a_i]_\rho) = o_j^*(f(a_i)).$$

因此 f 是由 V 到 V/ρ 的一个满同态.

14. 积代数

为简单起见,我们仅介绍两个代数系统的积代数.

设有代数系统 $V_1=\langle S_1; *_1, \sim_1\rangle$ 和 $V_2=\langle S_2; *_2, \sim_2\rangle$,其中 $*_i(i=1,2)$ 是二元运算,$\sim_i(i=1,2)$ 是一元运算. 利用集合 S_1 和 S_2 的笛卡尔积,可以构造一个新的代数系统 $V=\langle S; *, \sim\rangle$,称 V 为 V_1 和 V_2 的积代数. 又记 $V=V_1\times V_2$.

这里 $S=S_1\times S_2=\{(x_1,x_2)\mid x_1\in S_1, x_2\in S_2\}$.

$*$ 是二元运算,对于任意的 $(x_1,x_2),(y_1,y_2)\in S$,

$$(x_1,x_2)*(y_1,y_2) = (x_1 *_1 y_1, x_2 *_2 y_2).$$

$\sim$ 是一元运算,对于任意的 $(x_1,x_2)\in S$,

$$\sim(x_1,x_2) = (\sim_1(x_1), \sim_2(x_2)).$$

例 4-21 设 $V_1=\langle Z_2;\oplus_2\rangle$, $V_2=\langle Z_3;\oplus_3\rangle$,其中 $Z_2=\{0,1\}$, $Z_3=\{0,1,2\}$, $\oplus_2$ 和 $\oplus_3$ 分别是模 2 和模 3 的加法. 即

$$a\oplus_2 b = \mathrm{res}_2(a+b), \quad a\oplus_3 b = \mathrm{res}_3(a+b),$$

于是积代数

$$V_1 \times V_2 = \langle Z_2 \times Z_3; \oplus \rangle,$$

其中 $Z_2 \times Z_3 = \{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2)\}$.

运算$\oplus$的定义如表 4-3 所示.

表 4-3

$\oplus$	(0,0)	(0,1)	(0,2)	(1,0)	(1,1)	(1,2)
(0,0)	(0,0)	(0,1)	(0,2)	(1,0)	(1,1)	(1,2)
(0,1)	(0,1)	(0,2)	(0,0)	(1,1)	(1,2)	(1,0)
(0,2)	(0,2)	(0,0)	(0,1)	(1,2)	(1,0)	(1,1)
(1,0)	(1,0)	(1,1)	(1,2)	(0,0)	(0,1)	(0,2)
(1,1)	(1,1)	(1,2)	(1,0)	(0,1)	(0,2)	(0,0)
(1,2)	(1,2)	(1,0)	(1,1)	(0,2)	(0,0)	(0,1)

4.3 问答与论证

例 4-22 设$\langle S; * \rangle$是一代数系统，$*$是可结合的二元运算，且对于所有的 $x,y \in S$，若 $x * y = y * x$，则 $x = y$. 试证明 S 中每一个元素均是幂等元.

证 因为$*$可结合，所以对于任意的 $x \in S$，有

$$(x * x) * x = x * (x * x),$$

由题设条件 $x * x = x$，故 x 是幂等元，由 x 的任意性，S 中每一元素均是幂等元.

例 4-23 设有代数系统$\langle S; *, \circ \rangle$，其中$*$和$\circ$均是二元运算，并分别具有单位元 e_1 和 e_2. 已知运算$*$和$\circ$相互之间均是可分配的. 试证明对于 S 中任意的元素 x，有 $x * x = x \circ x = x$.

证 因为 e_1 是$*$的单位元，e_2 是$\circ$的单位元，所以

$$\begin{aligned} e_1 &= e_2 \circ e_1 = (e_2 * e_1) \circ e_1 = (e_2 \circ e_1) * (e_1 \circ e_1) \\ &= e_1 * (e_1 \circ e_1) = e_1 \circ e_1; \\ e_2 &= e_1 * e_2 = (e_1 \circ e_2) * e_2 = (e_1 * e_2) \circ (e_2 * e_2) \\ &= e_2 \circ (e_2 * e_2) = e_2 * e_2. \end{aligned}$$

于是,对于任意的 $x\in S$,有

$$x * x = (x \circ e_2) * (x \circ e_2) = x \circ (e_2 * e_2) = x \circ e_2 = x$$

$$x \circ x = (x * e_1) \circ (x * e_1) = x * (e_1 \circ e_1) = x * e_1 = x;$$

故对于任意 $x\in S$,有

$$x * x = x \circ x = x.$$

例 4-24 设 f_1 和 f_2 都是从代数系统 $\langle S_1; * \rangle$ 到 $\langle S_2; \circ \rangle$ 的同态,这里 $*$ 和 $\circ$ 都是二元运算,且 $\circ$ 是可交换和可结合的. 定义函数 $h: S_1 \to S_2$,使得对于任意 $x\in S_1$,$h(x)=f_1(x) \circ f_2(x)$. 试证明 h 也是从 $\langle S_1; * \rangle$ 到 $\langle S_2; \circ \rangle$ 的同态.

证 对于任意 $x,y\in S_1$,因为 f_1 和 f_2 都是从 $\langle S_1; * \rangle$ 到 $\langle S_2; \circ \rangle$ 的同态,所以有

$$\begin{aligned} h(x * y) &= f_1(x * y) \circ f_2(x * y) \\ &= (f_1(x) \circ f_1(y)) \circ (f_2(x) \circ f_2(y)). \end{aligned}$$

又因为 $\circ$ 是可交换和可结合的,所以

$$\begin{aligned} h(x * y) &= (f_1(x) \circ f_2(x)) \circ (f_1(y) \circ f_2(y)) \\ &= h(x) \circ h(y). \end{aligned}$$

由 x,y 的任意性,可知 h 也是从 $\langle S_1; * \rangle$ 到 $\langle S_2; \circ \rangle$ 的同态.

例 4-25 设 $V_1 = \langle C; +, \cdot \rangle$,其中 C 是复数集合,$+$ 和 $\cdot$ 是通常数的加法和乘法;$V_2 = \langle M; +, \circ \rangle$,其中

$$M = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \middle| a,b \in R \right\}$$

$+$ 和 $\circ$ 是矩阵的加法和乘法(R 是实数集). 试证明这两个代数系统同构.

证 定义函数 $h: C \to M$,对任意 $a+ib\in C$,

$$h(a+ib) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}.$$

对任意的 $a+ib, c+id\in C$,若 $a+ib \neq c+id$,则 $a\neq c$ 或 $b\neq d$,因此

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \neq \begin{bmatrix} c & d \\ -d & c \end{bmatrix},$$

即 $$h(a+ib) \neq h(c+id),$$

故 h 是内射.

对于任意$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in M$,显然$h(a+ib)=\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$,故 h 是满射,因此 h 是双射.

又对于任意的 $a+ib,c+id \in C$,

$$h((a+ib)+(c+id)) = h((a+c)+i(b+d))$$
$$= \begin{bmatrix} a+c & b+d \\ -(b+d) & a+c \end{bmatrix} = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \begin{bmatrix} c & d \\ -d & c \end{bmatrix}$$
$$= h(a+ib)+h(c+id).$$
$$h((a+ib)\cdot(c+id)) = h((ac-bd)+i(ad+cb))$$
$$= \begin{bmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{bmatrix} = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \cdot \begin{bmatrix} c & d \\ -d & c \end{bmatrix}$$
$$= h(a+ib)\cdot h(c+id).$$

由上可知 h 是从 V_1 到 V_2 的同构.

例 4-26 设 $f:A \to B$ 是从 $V_1=\langle A;\circ\rangle$到 $V_2=\langle B;*\rangle$的同态,$g:B \to C$ 是从 V_2 到 $V_3=\langle C;\times\rangle$的同态. 这里运算 $\circ$、$*$ 和 $\times$ 均是二元运算. 试证明复合函数 $g \cdot f:A \to C$ 是从 V_1 到 V_3 的同态.

证 因为 f 和 g 均是同态,所以对于任意的 $a_1,a_2 \in A$,有

$$g\cdot f(a_1 \circ a_2) = g(f(a_1 \circ a_2)) = g(f(a_1) * f(a_2))$$
$$= g\cdot f(a_1) \times g\cdot f(a_2),$$

故 $g\cdot f$ 是从 V_1 到 V_3 的同态.

例 4-27 设函数 $h:S_1 \to S_2$ 是从代数系统 $V_1=\langle S_1;*_1,\sim_1\rangle$到 $V_2=\langle S_2;*_2,\sim_2\rangle$的同态,其中运算 $*_i$ 和$\sim_i(i=1,2)$分别是二元运算和一元运算. 试证明 $h(S_1)$对于运算 $*_2$ 和$\sim_2$ 构成 V_2 的子代数.

分析 证明之前先要搞清楚符号$h(S_1)$的含义. $h(S_1)$是S_2的一个子集,由S_1中所有元素的像组成. 即

$$h(S_1)=\{y \mid y\in S_2, 存在 x\in S_1, 使 h(x)=y\}.$$

证 因为h是从S_1到S_2的函数,所以$h(S_1)\subseteq S_2$,且由S_1非空,可知$h(S_1)$也非空.

对于任意的$y_1,y_2\in h(S_1)$,必有$x_1,x_2\in S_1$,使得$h(x_1)=y_1$,$h(x_2)=y_2$,于是

$$y_1 *_2 y_2 = h(x_1) *_2 h(x_2) = h(x_1 *_1 x_2) = h(x)\in h(S_1)$$

对于任意$y\in h(S_1)$,必有$x\in S_1$,使得$h(x)=y$,于是

$$\sim_2(y)=\sim_2(h(x))=h(\sim_1(x))=h(x')\in h(S_1).$$

由y_1,y_2和y的任意性,运算$*_2$和$\sim_2$在子集$h(S_1)$上是封闭的. 故$\langle h(S_1);*_2,\sim_2\rangle$是$V_2$的子代数.

例 4-28 代数系统$V_1=\langle R-\{0\};\cdot\rangle$与$V_2=\langle R;+\rangle$同构吗? 其中$R$表示实数集,$\cdot$和$+$分别表示通常数的乘法和加法运算.

分析 如果V_1与V_2同构,则这两个代数系统应具有完全相同的性质. 例如V_1中有单位元1,V_2中有单位元0. 但是我们发现在V_1中元素-1满足等式$(-1)\cdot(-1)=1$,而在V_2中却找不出除单位元0以外的元素x,满足$x+x=0$. 因此V_1与V_2不可能同构. 下面给出这一结论的证明.

证 (反证法) 设存在函数$h:R-\{0\}\to R$是从V_1到V_2的同构,则由单位元映射为单位元,有$h(1)=0$.

又设$h(-1)=b$,则

$$h(1)=h((-1)\cdot(-1))=h(-1)+h(-1)=b+b.$$

因此$b+b=0$,即$b=0$,由此导致$h(1)=h(-1)$,这与h是双射相矛盾. 故$\langle R-\{0\};\cdot\rangle$与$\langle R;+\rangle$不同构.

若代数系统V_1和V_2是同一个代数系统V,则从V_1到V_2的同态称为V的自同态. 从V_1到V_2的同构称为V的自同构.

例 4-29 试证明代数系统$\langle Q;+,\cdot\rangle$上的自同构只有一个. 这里Q表示有理数集,$+$和$\cdot$分别表示通常数的加法和乘法运

算.

证 恒等函数 $I_Q:Q\to Q$ 显然是 $\langle Q;+,\cdot\rangle$ 上的一个自同构. 假设 h 也是 $\langle Q;+,\cdot\rangle$ 上的一个自同构,则由单位元映射为单位元知

$$h(0)=0,\quad h(1)=1.$$

对于任一正整数 m,由同态的定义,有

$h(m)=h(1+1+\cdots+1)=h(1)+h(1)+\cdots+h(1)=m.$

对于任一负整数 $-m$,因为 $-m$ 是 m 的加法逆元,由满同态的性质

$$h(-m)=-(h(m))=-m.$$

于是,对于任一非零整数 j,因为 $\frac{1}{j}$ 是 j 的乘法逆元,由满同态的性质

$$h(\frac{1}{j})=h(j^{-1})=(h(j))^{-1}=j^{-1}=\frac{1}{j}.$$

因此,对于任一有理数 q,设 $q=\frac{i}{j}$ (i,j 均是整数,且 $j\neq 0$),则 $i=q\cdot j$,且

$$h(i)=h(q\cdot j)=h(q)\cdot h(j).$$

于是

$$h(q)=\frac{h(i)}{h(j)}=\frac{i}{j}=q.$$

由上可知 $h=I_Q$,即 $\langle Q;+,\cdot\rangle$ 上的自同构只有一个.

例 4-30 设有代数系统 $\langle N;\cdot\rangle$ 和 $\langle\{0,1\};\cdot\rangle$. 其中 N 表示正整数集,$\cdot$ 表示通常数的乘法运算,函数 $h:N\to\{0,1\}$ 定义为

$$h(n)=\begin{cases}1, & n=2^k(k\geqslant 0),\\ 0; & \text{否则}\end{cases}$$

试证明 h 是从 $\langle N;\cdot\rangle$ 到 $\langle\{0,1\};\cdot\rangle$ 的同态.

证 对于任意的 $n_1,n_2\in N$.

(1) 若 $n_1=2^{k_1},n_2=2^{k_2}\quad(k_1,k_2\geqslant 0)$,则 $n_1\cdot n_2=2^{k_1+k_2}$,因此 $h(n_1\cdot n_2)=1,h(n_1)=1,h(n_2)=1$,

从而 $h(n_1 \cdot n_2)=h(n_1) \cdot h(n_2)$.

(2) 若 n_1 和 n_2 中至少有一个不能写成 2^k 的形式,例如设 n_1 不能写成 2^k 的形式,则必存在某奇数 p 使 $n_1=2^{k_1} \cdot p(p\neq 1)$,因为 $n_1 \cdot n_2$ 含有因子 p,所以也不能写成 2^k 的形式,于是 $h(n_1 \cdot n_2)=0, h(n_1)=0$,

且 $h(n_1) \cdot h(n_2)=0 \cdot h(n_2)=0$,

故
$$h(n_1 \cdot n_2) = h(n_1) \cdot h(n_2).$$

由上可知,h 是从 $\langle N; \cdot \rangle$ 到 $\langle \{0,1\}; \cdot \rangle$ 的同态.

例 4-31 设有代数系统 $V=\langle S; *, \sim \rangle$, $*$ 和 $\sim$ 分别是二元运算和一元运算. ρ_1 和 ρ_2 均是 V 上的同余关系. 试问 $\rho_1 \cap \rho_2$ 和 $\rho_1 \cup \rho_2$ 是 V 上的同余关系吗?

解 $\rho_1 \cap \rho_2$ 是 V 上的同余关系,其证明如下.

首先由第二章例 2-33 可知 $\rho_1 \cap \rho_2$ 是 S 上的等价关系.

对于任意 $x_1, y_1, x_2, y_2 \in S$,若 $x_1(\rho_1 \cap \rho_2)y_1, x_2(\rho_1 \cap \rho_2)y_2$,则
$$x_1\rho_1 y_1, x_1\rho_2 y_1 \quad 且 \quad x_2\rho_1 y_2, x_2\rho_2 y_2,$$
因为 ρ_1 和 ρ_2 均是 V 上的同余关系,所以
$$(x_1 * x_2)\rho_1(y_1 * y_2) \quad 且 \quad (x_1 * x_2)\rho_2(y_1 * y_2),$$
因此
$$(x_1 * x_2)(\rho_1 \cap \rho_2)(y_1 * y_2),$$
故 $\rho_1 \cap \rho_2$ 对于运算 $*$ 满足代换性质.

又对于任意 $x, y \in S$,若 $x(\rho_1 \cap \rho_2)y$,则有
$$x\rho_1 y \quad 且 \quad x\rho_2 y,$$
于是
$$(\sim x)\rho_1(\sim y) \quad 且 \quad (\sim x)\rho_2(\sim y),$$
因此
$$(\sim x)(\rho_1 \cap \rho_2)(\sim y),$$
故 $\rho_1 \cap \rho_2$ 对于运算 $\sim$ 也满足代换性质.

由上可知,$\rho_1 \cap \rho_2$ 是 V 上的同余关系.

$\rho_1 \cup \rho_2$ 不一定是 V 上的同余关系. 因为 $\rho_1 \cup \rho_2$ 可能不是 V 上的等价关系.(参见第二章例 2-33)

例 4-32 设有代数系统 $\langle I; +, \cdot \rangle$,其中 I 表示整数集,$+$ 和

$\cdot$ 是通常数的加法和乘法运算. 集 I 上的关系 ρ 定义为,当且仅当 $|i_1|=|i_2|$ 时,$i_1\rho i_2$. 试问 ρ 对于 $+$ 满足代换性质吗? 对于 $\cdot$ 呢?

解 对于任意 $x_1,x_2,y_1,y_2\in I$,若 $x_1\rho y_1,x_2\rho y_2$,则 $|x_1|=|y_1|,|x_2|=|y_2|$,但此时不一定有 $|x_1+x_2|=|y_1+y_2|$.

例如,设 $x_1=2,y_1=-2,x_2=y_2=3$,则显然有 $|x_1|=|y_1|$, $|x_2|=|y_2|$,

但
$$|x_1+x_2|\neq|y_1+y_2|,$$
故 ρ 对 $+$ 不满足代换性质. 显然,在 $|x_1|=|y_1|,|x_2|=|y_2|$ 时,有
$$|x_1\cdot x_2|=|x_1|\cdot|x_2|=|y_1|\cdot|y_2|=|y_1\cdot y_2|,$$
所以有 $(x_1\cdot x_2)\rho(y_1\cdot y_2)$,故 ρ 对于 $\cdot$ 满足代换性质.

例 4-33 设 $V=\langle I;\circ\rangle$,其中 I 是整数集,$\circ$ 是一元运算,定义为 $\circ(i)\doteq\text{res}_m(i^k)\ (m>0,k>0)$. I 上的关系 ρ 定义为,当且仅当 $\text{res}_m(i_1)=\text{res}_m(i_2)$ 时,$i_1\rho i_2$. 试问 ρ 是 $\langle I;\circ\rangle$ 上的同余关系吗?

分析 (符号 $\text{res}_m(i)$ 表示 i 被 m 除后的非负余数. 例如 $\text{res}_6(49)=1,\text{res}_6(-49)=5$.)

解 由 ρ 的定义,ρ 显然是 I 上的等价关系. 同时 ρ 也是 $\langle I;\circ\rangle$ 上的同余关系. 其证明如下.

对任意 $i_1,i_2\in I$,若 $i_1\rho i_2$,则 $\text{res}_m(i_1)=\text{res}_m(i_2)$.

令
$$i_1=pm+r,i_2=qm+r\quad(0\leqslant r<m),$$
则
$$i_1^k=(pm+r)^k=C_k^0(pm)^k+C_k^1(pm)^{k-1}r+\cdots+C_k^{k-1}(pm)r^{k-1}+C_k^kr^k;$$
$$i_2^k=(qm+r)^k=C_k^0(qm)^k+C_k^1(qm)^{k-1}r+\cdots+C_k^{k-1}(qm)r^{k-1}+C_k^kr^k,$$
因此
$$\circ(i_1)=\text{res}_m(i_1^k)=\text{res}_m(r^k),$$
$$\circ(i_2)=\text{res}_m(i_2^k)=\text{res}_m(r^k).$$
于是 $\circ(i_1)=\circ(i_2)$,由 ρ 的自反性,有 $\circ(i_1)\rho\circ(i_2)$,因此 ρ 对于 $\circ$ 满足代换性质,故 ρ 是 $\langle I;\circ\rangle$ 上的同余关系.

第五章　群

5.1　内容提要

1. 半群和独异点

- 半群；
- 独异点；
- 循环独异点；
- 子半群和子独异点.

2. 群

- 群；
- 循环群；
- 元素的周期与群的阶.

3. 群的基本性质

- 群的消去律；
- 元素运算后求逆元；
- 元素的周期.

4. 子群及其陪集

- 子群及其判别；
- 子群的陪集；
- 正规子群及其判别；
- 群中与子群相关的左(右)陪集分划；

• 拉格朗日定理.

5.2 基本知识点

1. 半群

一个非空集合 S 和定义在其上的一个二元运算 $*$ 可组成一个代数系统 $\langle S; *\rangle$. 若运算 $*$ 满足结合律，则称代数系统 $\langle S; *\rangle$ 为半群.

例 5-1 设 R 是实数集，R 上的二元运算 $\times$ 定义为，$a\times b=|a|\cdot b$（$\cdot$ 表示通常数的乘法运算），问 R 与运算 $\times$ 能否构成半群？

解 对于任意的 $a,b,c\in R$，有

$(a\times b)\times c=(|a|\cdot b)\times c=||a|\cdot b|\cdot c=|a|\cdot|b|\cdot c$,

$a\times(b\times c)=|a|\cdot(b\times c)=|a|\cdot(|b|\cdot c)=|a|\cdot|b|\cdot c$,

所以 $$(a\times b)\times c=a\times(b\times c),$$

故 $\langle R;\times\rangle$ 是一个半群.

2. 独异点

如果半群 $\langle S; *\rangle$ 中运算 $*$ 具有单位元，则称该半群为独异点.

例 5-2 考察例 5-1 中的半群 $\langle S; *\rangle$，它是否是一个独异点？

解 对任意的 $b\in S$，若 a 是左单位元，则

$$a\times b=|a|\cdot b=b.$$

要使上式成立，只有 $|a|=1$. 即 $a=1$ 或 $a=-1$. 因此 1 和 -1 均是运算 $\times$ 的左单位元.

对任意的 $a\in S$，若 b 是右单位元，则有

$$a\times b=|a|\cdot b=a.$$

当 $a>0$ 时，要使上式成立，必须 $b=1$.

当 $a<0$ 时，要使上式成立，必须 $b=-1$.

因此，1 和 -1 均不能成为运算 $\times$ 的右单位元. 于是运算 $\times$ 不存在单位元. 故半群 $\langle S;*\rangle$ 不是独异点.

例 5-3 设 $A=\{0,1,2,3\}$，$\odot_4$ 为模 4 乘法. 即

$$a\odot_4 b=\mathrm{res}_4(a\cdot b),$$

试问 A 和 $\odot_4$ 能否构成独异点?

解 构造模 4 乘法在 A 上的运算表(表 5-1). 显然运算结果均是 A 中的元素，所以 $\langle A;\odot_4\rangle$ 构成一代数系统.

表 5-1

$\odot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

对于任意的 $a,b,c\in A$，令

$$a\cdot b=4m_1+\mathrm{res}_4(a\cdot b),b\cdot c=4m_2+\mathrm{res}_4(b\cdot c),$$

则 $$(a\odot_4 b)\odot_4 c=\mathrm{res}_4(a\cdot b)\odot_4 c=\mathrm{res}_4((\mathrm{res}_4(a\cdot b))\cdot c)$$
$$=\mathrm{res}_4((4m_1+\mathrm{res}_4(a\cdot b))\cdot c)$$
$$=\mathrm{res}_4((a\cdot b)\cdot c),$$

$$a\odot_4(b\odot_4 c)=a\odot_4\mathrm{res}_4(b\cdot c)=\mathrm{res}_4(a\cdot\mathrm{res}_4(bc))$$
$$=\mathrm{res}_4(a\cdot(4m_2+\mathrm{res}_4(b\cdot c)))=\mathrm{res}_4(a\cdot(b\cdot c)).$$

因为通常数的乘法运算 · 是可结合的，所以

$$(a\odot_4 b)\odot_4 c=a\odot_4(b\odot_4 c),$$

即 $\odot_4$ 满足结合律.

由运算表可看出，1 是 $\odot_4$ 的左单位元，也是右单位元，因此 1 是 $\odot_4$ 的单位元. 故 $\langle A;\odot_4\rangle$ 是一独异点.

3. 循环独异点

在半群或独异点 $\langle S;*\rangle$ 中，运算 $*$ 是可结合的，因此可以对

任意的 $a\in S$，定义 a^n 为：

$$a^1 = a;$$

$$a^{n+1} = a^n * a \quad (n \text{ 为任意正整数}).$$

对于独异点，又可规定 $a^0=e$ （e 表示单位元）.

用数学归纳法不难证明 a 的幂遵从以下规律

$$a^n * a^m = a^{n+m}, \quad (a^n)^m = a^{nm}.$$

以上两式，对于半群来说，m 和 n 为任意正整数；对于独异点来说，m 和 n 为任意非负整数.

在独异点 $\langle S;*\rangle$ 中，如果存在一个元素 g，使得 S 中的每一个元素 a 均可表示成 $a=g^i$（i 为非负整数），则称 $\langle S;*\rangle$ 为循环独异点，称 g 为 $\langle S;*\rangle$ 的生成元.

例 5-4 考察例 5-3 中的独异点是否为循环独异点？

解 例 5-3 中的独异点 $\langle A;\odot_4\rangle$ 不是循环独异点. 因为 A 中不存在元素 g 能满足循环独异点的定义条件.

例如，$0^0=1, 0^1=0^2=0^3=\cdots=0$；

$1^0=1^1=1^2=1^3=\cdots=1$；$2^0=1, 2^1=2$，

$2^2=2^3=2^4=\cdots=0$；$3^1=3^3=3^5=\cdots=3$，

$3^0=3^2=3^4=\cdots=1$.

例 5-5 设 $V=\langle\{a,b,c,d\};*\rangle$，其中运算 $*$ 由表 5-2 定义

表 5-2

*	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

试问 V 是循环独异点吗？若是，请指出它的生成元.

解 根据运算表，用枚举法可以证明，对于任意 $x,y,z\in\{a,b,c,d\}$，等式 $(x*y)*z=x*(y*z)$ 是成立的. 因为证明过程太繁琐，这里省略.

由运算表可以看出 a 是单位元，因此 V 是一独异点.

因为 $b^1=b, b^2=c, b^3=c*b=d, b^4=d*b=a$，所以 V 是一循环独异点. b 是其生成元. 另外，

由于 $\quad d^1=d, d^2=c, d^3=c*d=b, d^4=b*d=a$

因此 d 也是 V 的生成元.

a 和 c 不是 V 的生成元，读者可根据生成元的定义自己验证.

4. 子半群和子独异点

设 $\langle S; * \rangle$ 是一个半群，如果 S 的非空子集 T 使得运算 $*$ 在 T 上封闭，那么 $\langle T; * \rangle$ 就构成 $\langle S; * \rangle$ 的子代数. 我们称 $\langle T; * \rangle$ 是 $\langle S; * \rangle$ 的子半群. 因为运算 $*$ 在 T 上也是可结合的，所以子半群也是一个半群.

若 $\langle S; * \rangle$ 是一个独异点，$\langle T; * \rangle$ 是 $\langle S; * \rangle$ 的子代数，并且 $\langle S; * \rangle$ 的单位元 $e \in T$，则称 $\langle T; * \rangle$ 是 $\langle S; * \rangle$ 的子独异点. 显然子独异点也是一个独异点.

例 5-6 设 $S=\left\{\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \middle| a,b \in R\right\}$（$R$ 是实数集），$\cdot$ 是矩阵的乘法运算，则 $\langle S; \cdot \rangle$ 是一个半群. 因为矩阵 $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ 是其单位元，所以 $\langle S; \cdot \rangle$ 也是一个独异点. 设

$$T=\left\{\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \middle| a \in R\right\},$$

则 $T \subseteq S$，且 $\cdot$ 在 T 上封闭，所以 $\langle T; \cdot \rangle$ 是 $\langle S; \cdot \rangle$ 的子半群.

在 $\langle T; \cdot \rangle$ 中，$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ 是单位元，所以 $\langle T; \cdot \rangle$ 是一独异点. 但因为 $\langle S; \cdot \rangle$ 的单位元 $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \notin T$，所以 $\langle T; \cdot \rangle$ 不是 $\langle S; \cdot \rangle$ 的子独异点. 设

$$H=\left\{\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \middle| a \in R\right\},$$

则 $H\subseteq S$，且 $\cdot$ 在 H 上是封闭的，所以 $\langle H;\cdot\rangle$ 是 $\langle S;\cdot\rangle$ 的子半群. 因为单位元 $\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}\in H$，所以 $\langle H;\cdot\rangle$ 是 $\langle S;\cdot\rangle$ 的子独异点.

5. 群

如果独异点 $\langle G;*\rangle$ 中，每一元素均有逆元，则称 $\langle G;*\rangle$ 是一个群. 我们常将元素 a 的逆元记作 a^{-1}. 因此在群 $\langle G;*\rangle$ 中，若 $a\in G$，则必存在一元素 $a^{-1}\in G$，使得 $a*a^{-1}=a^{-1}*a=e$.

例 5-7 设 $G=Q-\{1\}$（Q 为有理数集），定义 G 上的二元运算 $*$ 为 $a*b=a+b-ab$. 试问 $\langle G;*\rangle$ 是群吗？

解 对任意的 $a,b,c\in G$，

$$\begin{aligned}(a*b)*c &= (a+b-ab)*c\\ &= a+b-ab+c-(a+b-ab)c\\ &= a+b+c-ab-ac-bc+abc;\\ a*(b*c) &= a*(b+c-bc)\\ &= a+b+c-bc-a(b+c-bc)\\ &= a+b+c-bc-ab-ac+abc;\end{aligned}$$

所以
$$(a*b)*c=a*(b*c),$$

又对于任意 $a\in G$，$0*a=a*0=a$，所以 0 是 $\langle G;*\rangle$ 的单位元.

对任意 $a\in G$，有 $a*\frac{a}{a-1}=\frac{a}{a-1}*a=0$. 所以每一元素 a 均有逆元，其逆元为 $\frac{a}{a-1}$.

由上可知 $\langle G;*\rangle$ 是一个群.

若将集合 $G=Q-\{1\}$ 改为 $G=Q$，则 $\langle Q;*\rangle$ 不是群. 因为 1 没有逆元，不符合群的定义.

6. 循环群

类似于独异点，在群 $\langle G;*\rangle$ 中也可定义元素 a 的幂为

$$a^0=e;$$

$$a^{n+1} = a^n * a \quad (n \text{ 为任意非负整数}).$$

由于群中每一元素都有逆元,因此又有

$$a^{-n} = (a^{-1})^n.$$

因为等式 $a^n * a^m = a^{n+m}$ 和 $(a^n)^m = a^{nm}$

仍然成立,所以又有 $a^{-n} = (a^n)^{-1}$.

类似于独异点,我们也可以引入循环群的概念.

在群 $\langle G;*\rangle$ 中,如果存在一个元素 g,使得 G 中每一个元素 a 均可表示成 $a=g^i$(i 是整数),则称 $\langle G;*\rangle$ 为循环群,称 g 为 $\langle G;*\rangle$ 的生成元.

例 5-8 设有代数系统 $\langle I;\circ\rangle$,其中 I 为整数集,运算 $\circ$ 定义为,对于任意 $a,b\in I$,

$$a\circ b = a + b - 2.$$

试问 $\langle I;\circ\rangle$ 是否为循环群?

解 对任意 $a,b,c\in I$,

$$\begin{aligned}(a\circ b)\circ c &= (a+b-2)\circ c \\ &= a+b-2+c-2 = a+b+c-4;\\ a\circ(b\circ c) &= a\circ(b+c-2) \\ &= a+b+c-2-2 = a+b+c-4;\end{aligned}$$

因此 $$(a\circ b)\circ c = a\circ(b\circ c).$$

又对于任意的 $a\in I$,$a\circ 2=a+2-2=a$ 且运算 $\circ$ 是可交换的,所以有单位元 2.

对任意 $a\in I$,若 $a\circ b=a+b-2=2$,则 $b=4-a$. 因此每一元素 a 均有逆元 $a^{-1}=4-a$.

由上可知 $\langle I;\circ\rangle$ 是一个群.

$\langle I;\circ\rangle$ 也是一循环群. 生成元是 1,不难验证,对于任意整数 n,$1^n=2-n$. 因此对于任意整数 n,$n=1^{2-n}$. 3 也是生成元,对于任意整数 n,$3^n=n+2$.

7. 元素的周期与群的阶

在群 $\langle G;*\rangle$ 中,元素 a 的周期是指这样的一个正整数 r,它使

得 $a^r=e$，且 r 是使得这一等式成立的最小的正整数. 如果对元素 a，不存在这样的正整数 r，则称 a 具有无限的周期.

群 $\langle G;*\rangle$ 的阶定义为集合 G 中元素的个数，根据它是有限或无限，可将群 $\langle G;*\rangle$ 分为有限群和无限群.

例 5-9 设有群 $\langle Z_6;\oplus_6\rangle$，其中 $Z_6=\{0,1,2,3,4,5\}$，$\oplus_6$ 是模 6 加法，即对于任意的 $a,b\in Z_6$，$a\oplus_6 b=\mathrm{res}_6(a+b)$. 试求出群 $\langle Z_6;\oplus_6\rangle$ 的阶和群中每一元素的周期.

解 因为 Z_6 的元素个数是 6，所以群 $\langle Z_6;\oplus_6\rangle$ 的阶为 6.

0 是单位元，所以 0 的周期是 1.

$1^1=1$，$1^2=1\oplus_6 1=2$，$1^3=1^2\oplus_6 1=2\oplus_6 1=3$，$1^4=1^3\oplus_6 1=3\oplus_6 1=4$，$1^5=1^4\oplus_6 1=4\oplus_6 1=5$，$1^6=1^5\oplus_6 1=5\oplus_6 1=0$，所以 1 的周期是 6.

$2^1=2$，$2^2=2\oplus_6 2=4$，$2^3=2^2\oplus_6 2=4\oplus_6 2=0$，所以 2 的周期是 3.

$3^1=3$，$3^2=3\oplus_6 3=0$，所以 3 的周期是 2.

$4^1=4$，$4^2=4\oplus_6 4=2$，$4^3=2\oplus_6 4=0$，所以 4 的周期是 3.

$5^1=5$，$5^2=5\oplus_6 5=4$，$5^3=4\oplus_6 5=3$，$5^4=3\oplus_6 5=2$，$5^5=2\oplus_6 5=1$，$5^6=1\oplus_6 5=0$，所以 5 的周期是 6.

由上也可看出，群 $\langle Z_5;\oplus_6\rangle$ 是一循环群. 1 或 5 是其生成元，且生成元的周期与循环群 $\langle G;*\rangle$ 的阶相等.

群有许多重要的性质，下面 8、9、10 款中列出了群的一些基本性质，并举出了一些例子. 希望读者通过这些例子理解并熟悉群的性质.

8. 群的消去律

若 $\langle G;*\rangle$ 是一个群，则对任意的 $a,b\in G$，方程 $a*x=b$ 和 $*a=b$ 在 G 中均存在唯一的解. 由此可以推出，对于任意 a,b,c G，若 $a*b=a*c$，则 $b=c$；若 $b*a=c*a$，则 $b=c$. 这一性质称是群的消去律.

例 5-10 试证明在一个群$\langle G;*\rangle$中，如果对于任意的$a,b\in G$，有$(a*b)^2=a^2*b^2$，则$\langle G;*\rangle$必是交换群.

证 因为对于任意的$a,b\in G$，有

$$(a*b)*(a*b)=(a*a)*(b*b),$$

$$a*(b*a)*b=a*(a*b)*b,$$

于是根据消去律$b*a=a*b$，故$\langle G;*\rangle$是一交换群.

9. 群中元素运算后求逆元

设$\langle G;*\rangle$是一个群，则对任意的$a_1,a_2,\cdots,a_n\in G$，有

$$(a_1*a_2*\cdots*a_n)^{-1}=a_n^{-1}*a_{n-1}^{-1}*\cdots*a_1^{-1}$$

例 5-11 设$\langle G;*\rangle$是一个独异点，且对于任意的$a\in G$，均有$a*a=e$. 试证明$\langle G;*\rangle$是交换群.

证 因为对于任意$a\in G$，均有$a*a=e$，所以任意元素a均有逆元，且$a^{-1}=a$. 因此$\langle G;*\rangle$是一个群. 于是对于任意的$a,b\in G$，有

$$a*b=(a*b)^{-1}.$$

又根据上述群的性质$(a*b)^{-1}=b^{-1}*a^{-1}$，因此

$$a*b=b^{-1}*a^{-1}=b*a,$$

故$\langle G;*\rangle$是一交换群.

10. 群中元素的周期

与群中元素周期有关的有如下一些性质.

设$\langle G;*\rangle$是一个群

(1) 若元素$a\in G$具有有限周期r，则当且仅当k是r的整数倍时，$a^k=e$.

(2) 群中任一元素a与它的逆元a^{-1}具有相同的周期.

(3) 若$\langle G;*\rangle$是有限群，则G中每个元素均具有有限的周期，且每个元素的周期是$\#G$的因子.（$\#G$表示集合G的基数，即群$\langle G;*\rangle$的阶）

(4) 设$\langle G; * \rangle$是一由元素 g 生成的循环群.

如果 g 的周期为 n,那么$\langle G; * \rangle$的阶为 n.

如果 g 的周期为无限,那么$\langle G; * \rangle$的阶为无限.

例 5-12 试证明在一个有限群中,周期大于 2 的元素个数一定是偶数.

证 设$\langle G; * \rangle$是一有限群,又设 $a \in G$ 是 G 中周期大于 2 的元素. 于是 $a \neq e$ 且 $a^2 \neq e$,又由 $a * a^{-1} = e$ 可知 $a \neq a^{-1}$. 而 a^{-1}与 a 的周期是相同的,于是由群中逆元的唯一性,群$\langle G; * \rangle$中周期大于 2 的元素必成对出现,因此其个数必为偶数.

例 5-13 试证明在阶为偶数的有限群中,周期等于 2 的元素个数一定是奇数.

证 设$\langle G; * \rangle$是一阶为偶数的有限群,由例 5-12 知 G 中周期大于 2 的元素个数是偶数. 又单位元 e 是群中唯一周期为 1 的元素,于是由 G 中元素个数为偶数,知 G 中周期为 2 的元素必存在且个数为奇数.

例 5-14 例 5-9 中群$\langle Z_6; \oplus_6 \rangle$的阶为 6,$G$ 中每一元素的周期均是 6 的因子. 1 和 5 互为逆元,其周期均为 6;2 和 4 互为逆元,其周期均为 3;3 以自身为逆元,其周期为 2. 单位元 0 的周期为 1. $\langle Z_6; \oplus_6 \rangle$是一循环群,生成元 1 和 5 的周期与群的阶相等.

群$\langle Z_6; \oplus_6 \rangle$中周期大于 2 的元素个数是 4 个. 它们分别是 1、5、2、4. 周期等于 2 的元素个数是 1 个,仅元素 3.

设 $V_1 = \langle S_1; * \rangle$和 $V_2 = \langle S_2; \circ \rangle$是两个代数系统,$f$ 是从 V_1 到 V_2 的同态. 如果 f 不是满同态,那么 S_1 关于 $*$ 的单位元 e_1 通过 f 映射的像不一定是 S_2 关于 $\circ$ 的单位元. S_1 中任一元素 a 的逆元 a^{-1}通过 f 映射的像 $f(a^{-1})$ 不一定是 $f(a)$的逆元. 但是,若 V_1 和 V_2 这两个代数系统都是群,则情形就不一样了.

例 5-15 设 f 是由群$\langle G_1; * \rangle$到群$\langle G_2; \circ \rangle$的同态,$e_1$ 和 e_2 分别是这两个群的单位元,则

(1) $f(e_1) = e_2$;

(2) 对任意的 $a \in G$，有 $f(a^{-1})=(f(a))^{-1}$.

证 (1) 因为 f 是同态，所以 $f(e_1)=f(e_1 * e_1)=f(e_1) \circ f(e_1)$. 即 $f(e_1)$ 是 $\langle G_2; \circ \rangle$ 中的幂等元. 但群中除单位元外，没有其它任何幂等元，因此 $f(e_1)=e_2$. 下面给出这一结论的证明：

$$
\begin{aligned}
f(e_1) &= e_2 \circ f(e_1) \\
&= ((f(e_1))^{-1} \circ f(e_1)) \circ f(e_1) \\
&= (f(e_1))^{-1} \circ (f(e_1) \circ f(e_1)) \\
&= (f(e_1))^{-1} \circ f(e_1) = e_2.
\end{aligned}
$$

(2) 对于任意 $a \in G_1$，

$$f(e_1) = f(a * a^{-1}) = f(a) \circ f(a^{-1}) = e_2.$$

又 $f(a) \circ (f(a))^{-1}=e_2$，因此

$$f(a) \circ f(a^{-1}) = f(a) \circ (f(a))^{-1}.$$

由群的消去律 $\qquad f(a^{-1})=(f(a))^{-1}$.

11. 子群的定义

设 $\langle G; * \rangle$ 是一个群，H 是 G 的一个非空子集，如果运算 $*$ 在 H 上封闭，则 $\langle H; * \rangle$ 构成 $\langle G; * \rangle$ 的子代数. 如果又有单位元 $e \in H$，且对于任意 $a \in H$，有 $a^{-1} \in H$，那么 $\langle H; * \rangle$ 称为群 $\langle G; * \rangle$ 的子群.

根据子群的定义，群 $\langle G; * \rangle$ 中 G 的非空子集 H 关于运算 $*$ 要能构成 $\langle G; * \rangle$ 的子群，H 必须满足以下三个条件：

(1) 封闭性：由 $a,b \in H$ 可推出 $a * b \in H$；

(2) 单位元 $e \in H$；

(3) 可逆性：由 $a \in H$ 可推出 $a^{-1} \in H$.

例 5-16 整数集 I 和数的加法运算构成的群 $\langle I; + \rangle$ 称为整数加群. 令 $H=\{3k \mid k \in I\}$，试问 H 和运算 $+$ 能否构成 $\langle I; + \rangle$ 的子群?

解 对于任意 $3k_1, 3k_2 \in H (k_1, k_2 \in I)$，因为 $3k_1+3k_2=3(k_1+k_2) \in H$，所以运算 $+$ 在 H 上是封闭的. 因此 $\langle H; + \rangle$ 是 $\langle I; + \rangle$ 的

子代数.

又$\langle I;+\rangle$的单位元是0,显然$0\in H$.对于任意$3k\in H$,其逆元$-3k=3\cdot(-k)\in H$.

故$\langle H;+\rangle$是群$\langle I;+\rangle$的子群.

例 5-17 设$\langle G;*\rangle$是一个群,定义G的子集H为

$$H=\{a\mid a*x=x*a,\text{对于任意的 } x\in G\},$$

试问H对于运算$*$能否构成$\langle G;*\rangle$的子群?

解 对于任意$x\in G$,显然有$e*x=x*e=x$,所以单位元$e\in H$且H非空.

设$a,b\in H$,则对于任意的$x\in G$,有

$$a*x=x*a,b*x=x*b.$$

于是 $(a*b)*x=a*(b*x)=(a*x)*b=x*(a*b)$.

因此$a*b\in H$.故$\langle H;*\rangle$是$\langle G;*\rangle$的子代数.

设$a\in H$,则由$a*x=x*a$,有

$$a^{-1}*(a*x)*a^{-1}=a^{-1}*(x*a)*a^{-1}.$$

因此$x*a^{-1}=a^{-1}*x$.于是$x^{-1}\in H$.

由上可知$\langle H;*\rangle$是群$\langle G;*\rangle$的子群.

12. 子群的判别方法

实际上,根据子群的判别定理判别时,可将定义中的判别条件简化.例如,可将封闭性和可逆性的证明可合并成一条来代替,由$a,b\in H$推出$a*b^{-1}\in H$.也就是说,对于群$\langle G;*\rangle$的任一非空子集H,若由$a,b\in H$,可推出$a*b^{-1}\in H$,则$\langle H;*\rangle$是$\langle G;*\rangle$的子群.在这里,单位元$e\in H$这一条件也不是必要的,因为它可以由封闭性和可逆性推出来,但我们往往通过证明$e\in H$来说明H是非空的.

例 5-18 设$\langle H_1;*\rangle$和$\langle H_2;*\rangle$是群$\langle G;*\rangle$的两个子群.试证明$H_1\cap H_2$对于运算$*$也构成$\langle G;*\rangle$的子群.

证 因为单位元$e\in H_1,e\in H_2$,所以$e\in H_1\cap H_2$.因此$H_1\cap$

H_2 非空.

设 $a,b\in H_1\cap H_2$，则 $a\in H_1,a\in H_2$ 且 $b\in H_1,b\in H_2$，由于 $\langle H_1;*\rangle$ 和 $\langle H_2;*\rangle$ 都是 $\langle G;*\rangle$ 的子群，因此 $b^{-1}\in H_1,b^{-1}\in H_2$，且 $a*b^{-1}\in H_1,a*b^{-1}\in H_2$，于是 $a*b^{-1}\in H_1\cap H_2$. 故 $\langle H_1\cap H_2;*\rangle$ 是 $\langle G;*\rangle$ 的子群.

例 5-19 设 f 和 g 都是由群 $\langle G_1;*\rangle$ 到群 $\langle G_2;\circ\rangle$ 的同态，令

$$H=\{a|a\in G_1,f(a)=g(a)\},$$

试证明 H 对于运算 $*$ 构成 $\langle G_1;*\rangle$ 的子群.

证 f 和 g 都是由群 $\langle G_1;*\rangle$ 到群 $\langle G_2;\circ\rangle$ 的同态，由例 5-15 可知 $f(e_1)=g(e_1)=e_2$（e_1 和 e_2 分别是 $\langle G_1;*\rangle$ 和 $\langle G_2;\circ\rangle$ 的单位元），因此 $e_1\in H$，H 非空.

设 $a,b\in H$，则 $f(a)=g(a)$，$f(b)=g(b)$，又由例 5-15 知，$f(b^{-1})=(f(b))^{-1}$，$g(b^{-1})=(g(b))^{-1}$，于是

$$\begin{aligned}f(a*b^{-1})&=f(a)\circ f(b^{-1})=f(a)\circ(f(b))^{-1}\\&=g(a)\circ(g(b))^{-1}\\&=g(a)\circ g(b^{-1})=g(a*b^{-1}).\end{aligned}$$

因此 $a*b^{-1}\in H$. 故 $\langle H;*\rangle$ 是群 $\langle G_1;*\rangle$ 的子群.

若 $\langle G;*\rangle$ 是一有限群，或者 $\langle G;*\rangle$ 是一个任意的群，但 H 是 G 的有限子集，那么只要运算 $*$ 在 H 上封闭，$\langle H;*\rangle$ 便是 $\langle G;*\rangle$ 的子群.

例 5-20 试对例 5-9 中的群 $\langle Z_6;\oplus_6\rangle$，找出它的所有子群.

解 因为群 $\langle Z_6;\oplus_6\rangle$ 是一阶为 6 的有限群，所以只要找出对运算 $\oplus_6$ 封闭的子集. 根据这一判别条件，$\langle Z_6;\oplus_6\rangle$ 有如下子群：

(1) $\langle\{0\};\oplus_6\rangle$；

(2) $\langle\{0,3\};\oplus_6\rangle$；

(3) $\langle\{0,2,4\};\oplus_6\rangle$；

(4) $\langle Z_6;\oplus_6\rangle$.

例 5-21 非零实数集 $R-\{0\}$ 对于通常数的乘法运算构成群 $\langle R-\{0\};\cdot\rangle$. 集合 $\{-1,1\}$ 是 $R-\{0\}$ 的有限子集，且运算 $\cdot$ 在 $\{-$

1,1}上是封闭的，因此⟨{−1,1}；·⟩是群⟨R−{0}；·⟩的子群.

13. 子群的陪集

设⟨H；$*$⟩是群⟨G；$*$⟩的子群，对任意的 $a\in G$，称集合 $a*H=\{a*h \mid h\in H\}$ 为子群⟨H；$*$⟩关于元素 a 的左陪集；称集合 $H*a=\{h*a \mid h\in H\}$ 为子群⟨H；$*$⟩关于元素 a 的右陪集.

子群⟨H；$*$⟩对于 G 中的每一个元素都可相应产生一个右陪集和左陪集. 但不同的元素所产生的左(右)陪集，可能是相同的.

例 5-22 例 5-21 中群⟨$R-\{0\}$；·⟩的子群⟨$\{-1,1\}$；·⟩关于1、2、3以及关于−1、−2、−3的左陪集如下：

$1\cdot\{-1,1\}=\{-1,1\}$；　　$-1\cdot\{-1,1\}=\{1,-1\}$；

$2\cdot\{-1,1\}=\{-2,2\}$；　　$-2\cdot\{-1,1\}=\{2,-2\}$；

$3\cdot\{-1,1\}=\{-3,3\}$；　　$-3\cdot\{-1,1\}=\{3,-3\}$.

由上可以看出，对于任意非零实数 a，子群⟨$\{-1,1\}$；·⟩关于 a 和关于 $-a$ 的左陪集是相等的. 即对于任意 $a\in R-\{0\}$，有 $a\cdot\{-1,1\}=-a\cdot\{-1,1\}$.

因为运算·是可交换的，所以对于任意 $a\in R-\{0\}$，又有

$$a\cdot\{-1,1\}=\{-a,a\},\{-1,1\}\cdot a=\{-a,a\},$$

因此子群⟨$\{-1,1\}$；·⟩关于元素 a 的左陪集和右陪集是相等的，即对于任意的 $a\in R-\{0\}$，有 $a\cdot\{-1,1\}=\{-1,1\}\cdot a$.

例 5-23 列出例 5-9 中群⟨Z_6；$\oplus_6$⟩的子群⟨$\{0,2,4\}$；$\oplus_6$⟩的所有右陪集.

解 $\{0,2,4\}\oplus_6 0=\{0,2,4\}$；

$\{0,2,4\}\oplus_6 1=\{1,3,5\}$；

$\{0,2,4\}\oplus_6 2=\{2,4,0\}$；

$\{0,2,4\}\oplus_6 3=\{3,5,1\}$；

$\{0,2,4\}\oplus_6 4=\{4,0,2\}$；

$\{0,2,4\}\oplus_6 5=\{5,1,3\}$.

由上看出

$$\{0,2,4\}\oplus_6 0=\{0,2,4\}\oplus_6 2=\{0,2,4\}\oplus_6 4;$$
$$\{0,2,4\}\oplus_6 1=\{0,2,4\}\oplus_6 3=\{0,2,4\}\oplus_6 5.$$
因此子群$\langle\{0,2,4\};\oplus_6\rangle$在群$\langle Z_6;\oplus_6\rangle$中只有两个不同的右陪集.

14. 正规子群

设$\langle H;*\rangle$是群$\langle G;*\rangle$的子群,如果对于每一个$a\in G$,都有$a*H=H*a$,则称$\langle H;*\rangle$是$\langle G;*\rangle$的正规子群,此时$a*H$或$H*a$就简称作是子群$\langle H;*\rangle$关于元素a的陪集.

例如,例5-22和例5-23中群$\langle R-\{0\};\cdot\rangle$和群$\langle Z_6;\oplus_6\rangle$都是交换群,因此它们的每一个子群都是正规子群

下面看一个非交换群的例子.

设集合$A=\{a_1,a_2,\cdots,a_n\}$是一有限集,从A到A的双射函数称为是A上的置换. n称为置换的阶. 一个n阶置换$f:A\to A$常表示成如下形式:

$$f=\begin{bmatrix} a_1 & a_2 & \cdots & a_n \\ f(a_1) & f(a_2) & \cdots & f(a_n) \end{bmatrix}.$$

例5-24 若集合$A=\{a,b,c\}$,则从A到A的双射函数称为是A上的3阶置换. 这样的置换共有$3!=6$个. 它们是

$$1=\begin{bmatrix} a & b & c \\ a & b & c \end{bmatrix},\quad \alpha=\begin{bmatrix} a & b & c \\ a & c & b \end{bmatrix},\quad \beta=\begin{bmatrix} a & b & c \\ b & a & c \end{bmatrix},$$
$$\gamma=\begin{bmatrix} a & b & c \\ b & c & a \end{bmatrix},\quad \delta=\begin{bmatrix} a & b & c \\ c & a & b \end{bmatrix},\quad \epsilon=\begin{bmatrix} a & b & c \\ c & b & a \end{bmatrix}.$$

令$P=\{1,\alpha,\beta,\gamma,\delta,\epsilon\}$,显然$P$对于函数的复合运算(也称作置换的复合运算)$\circ$是封闭的,所以构成代数系统$\langle P;\circ\rangle$.

因为函数的复合运算满足结合律,恒等函数(亦称为恒等置换)1是其单位元,P中任一双射函数的逆函数仍是A到A的双射,且它们复合运算后等于恒等函数. 因此每一置换均有逆元. 事实上,$1^{-1}=1,\alpha^{-1}=\alpha,\beta^{-1}=\beta,\gamma^{-1}=\delta,\delta^{-1}=\gamma,\epsilon^{-1}=\epsilon$. 因此$\langle P;\circ\rangle$是一个群. 其运算表如表5-3所示.

表5-3

$\circ$	1	α	β	γ	δ	ε
1	1	α	β	γ	δ	ε
α	α	1	γ	β	ε	δ
β	β	δ	1	ε	α	γ
γ	γ	ε	α	δ	1	β
δ	δ	β	ε	1	γ	α
ε	ε	γ	δ	α	β	1

注意运算表中 p 和 q 的复合 $p \circ q$ 是表示置换 p 后再置换 q 而产生的置换.例如

$$\alpha \circ \beta = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix} \circ \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix} \circ \begin{pmatrix} a & c & b \\ b & c & a \end{pmatrix}$$

$$= \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix} = \gamma.$$

这是一个有限群,通过检验子集对运算 $\circ$ 的封闭性可知,$\langle\{1,\alpha\};\circ\rangle$、$\langle\{1,\beta\};\circ\rangle$、$\langle\{1,\gamma,\delta\};\circ\rangle$、$\langle\{1,\varepsilon\};\circ\rangle$等都是$\langle\rho;\circ\rangle$的子群.但由于$\langle\rho;\circ\rangle$不是交换群,它的子群是否正规子群就需要具体验证等式 $a * H = H * a$ 是否对群中所有的元素 a 成立.经验证发现子群$\langle\{1,\alpha\};\circ\rangle$、$\langle\{1,\beta\};\circ\rangle$和$\langle\{1,\varepsilon\};\circ\rangle$均不是正规子群.而$\langle\{1,\gamma,\delta\};\circ\rangle$是正规子群.例如,对于子群$\langle\{1,\alpha\};\circ\rangle$,

$$\gamma \circ \{1,\alpha\} = \{\gamma,\varepsilon\}, \{1,\alpha\} \circ \gamma = \{\gamma,\beta\},$$

$\gamma \circ \{1,\alpha\} \neq \{1,\alpha\} \circ \gamma$,所以$\langle\{1,\alpha\};\circ\rangle$不是正规子群.

类似地,对于子群$\langle\{1,\beta\};\circ\rangle$,

$$\alpha \circ \{1,\beta\} = \{\alpha,\gamma\}, \{1,\beta\} \circ \alpha = \{\alpha,\delta\},$$

$\alpha \circ \{1,\beta\} \neq \{1,\beta\} \circ \alpha$.对于子群$\langle\{1,\varepsilon\};\circ\rangle$,

$$\gamma \circ \{1,\varepsilon\} = \{\gamma,\beta\}, \{1,\varepsilon\} \circ \gamma = \{\gamma,\alpha\}$$

$\gamma \circ \{1,\varepsilon\} \neq \{1,\varepsilon\} \circ \gamma$.

易证,对于任意 $a \in P$,均有

$$a \circ \{1,\gamma,\delta\} = \{1,\gamma,\delta\} \circ a.$$

例如，

$$a\circ\{1,\gamma,\delta\}=\{\alpha,\beta,\varepsilon\},\{1,\gamma,\delta\}\circ\alpha=\{\alpha,\varepsilon,\beta\}$$

$$\beta\circ\{1,\gamma,\delta\}=\{\beta,\varepsilon,\alpha\},\{1,\gamma,\delta\}\circ\beta=\{\beta,\alpha,\varepsilon\}.$$

对于其它元素的验证过程，留给读者自己完成. 因此$\langle\{1,\gamma,\delta\};\circ\rangle$是$\langle\rho;\circ\rangle$的正规子群.

15. 正规子群的判别方法

对于群$\langle G;*\rangle$的子群$\langle H;*\rangle$，如何判别$\langle H;*\rangle$是否为$\langle G;*\rangle$的正规子群呢？有如下三种方法：

(1) 根据正规子群的定义，如果对于每一个$a\in G$，都有$a*H=H*a$，则$\langle H;*\rangle$是群$\langle G;*\rangle$的正规子群.

(2) 如果对于每一个$a\in G$，都有$a*H*a^{-1}=H$，则$\langle H;*\rangle$是$\langle G;*\rangle$的正规子群.

(3) 如果对于每一个$a\in G$，都有$a*H*a^{-1}\subseteq H$，则$\langle H;*\rangle$是$\langle G;*\rangle$的正规子群.

上述方法中，当然第三种方法较为简单，因为它只要证明一个包含关系.

例如，在例 5-24 中，

$$\gamma\circ\{1,\alpha\}\circ\gamma^{-1}=\{\gamma,\varepsilon\}\circ\delta=\{1,\beta\}\not\subseteq\{1,\alpha\}$$

所以$\langle\{1,\alpha\};\circ\rangle$不是$\langle\rho;\circ\rangle$的正规子群.

例 5-25 设$\langle G;*\rangle$是一个群，定义G的子集H为

$$H=\{a\mid a*x=x*a,\text{对于任意的 }x\in G\}.$$

在例 5-17 中我们证明了$\langle H;*\rangle$是$\langle G;*\rangle$的子群. 实际上，$\langle H;*\rangle$也是$\langle G;*\rangle$的正规子群. 对此，我们只要证明对于任意的$b\in G$，$b*H*b^{-1}\subseteq H$即可.

证 因为对于任意的$a\in H$和任意的$b\in G$，

$$b*a*b^{-1}=b*(a*b^{-1})=b*(b^{-1}*a)=(b*b^{-1})*a$$
$$=e*a=a\in H,$$

所以，$b*H*b^{-1}\subseteq H$. 故$\langle H;*\rangle$是群$\langle G;*\rangle$的正规子群.

16. 群中与子群相关的左(右)陪集分划

若$\langle H; * \rangle$是群$\langle G; * \rangle$的子群，则对于G中的每一个元素a，相应有一个左陪集$a * H$. 这些左陪集中，所有相异的左陪集刚好构成G的一个分划. 而且由于$\# H = \#(a * H)$，所以这种分划的每一个分划块都具有相同的基数. 这一分划称为是与子群$\langle H; * \rangle$相关的左陪集分划.

对于$\langle H; * \rangle$的右陪集有完全类似的结论，所构成的分划称为是与子群$\langle H; * \rangle$相关的右陪集分划.

例 5-26 对于例 5-23 求出群$\langle Z_6; \oplus_6 \rangle$中与子群$\langle \{0,2,4\}; \oplus_6 \rangle$相关的右陪集分划和左陪集分划.

解 在例 5-23 中，已求出子群$\langle \{0,2,4\}; \oplus_6 \rangle$关于$Z_6$中每一元素的右陪集，我们发现它只有两个不同的右陪集. 这两个右陪集构成G的一个分划. 因此与子群$\langle \{0,2,4\}; \oplus_6 \rangle$相关的右陪集分划

$$\Pi = \{\{0,2,4\}, \{1,3,5\}\} .$$

因为$\langle Z_6; \oplus_6 \rangle$是交换群，对于任意$a \in Z_6$，均有$a \oplus_6 \{0,2,4\} = \{0,2,4\} \oplus_6 a$，所以与子群$\langle \{0,2,4\}; \oplus_6 \rangle$相关的左陪集分划也是$\Pi$.

例 5-27 对于群$\langle Q^*; \cdot \rangle$(其中$Q^*$为非零有理数集，$\cdot$是通常数的乘法)，若令$H = \{-1,1\}$，则$\langle H; \cdot \rangle$构成$\langle Q^*; \cdot \rangle$的子群. 试求出子群$\langle H; \cdot \rangle$的所有左陪集.

解 对于每一个正有理数q，相应的左陪集

$$q \cdot H = q \cdot \{-1,1\} = \{-q, q\}.$$

对于每一个负有理数$-q$，相应的左陪集

$$-q \cdot H = -q \cdot \{-1,1\} = \{q, -q\};$$

因此有

$$q \cdot H = -q \cdot H.$$

但对于任意两个正有理数q_1和q_2，若$q_1 \neq q_2$，则

$$q_1 \cdot H \neq q_2 \cdot H.$$

因此$\langle H;*\rangle$的所有左陪集由每一个$q\in Q^+$(Q^+表示正有理数集)相关的左陪集$q\cdot H=\{-q,q\}$组成.这些左陪集构成Q^*的一个分划.即

$$\Pi=\{q\cdot H|q\in Q^+\}.$$

因为运算·是可交换的,对于每一个$a\in Q^*$,$a*H=H*a$,所以上述与子群$\langle H;*\rangle$相关的左陪集分划Π,也是与$\langle H;\cdot\rangle$相关的右陪集分划.每一个分划块都由2个元素组成.

例5-28 对于群$\langle Q;+\rangle$(其中Q为有理数集,+为通常数的加法运算),若令I为所有整数的集合,则$\langle I;+\rangle$构成$\langle Q;+\rangle$的子群,试求出子群$\langle I;+\rangle$的所有右陪集.

解 任意两个相邻的整数i与$i+1$之间都有无穷多个有理数.在区间$[0,1)$内任取一有理数a,则

$$\cdots-3+a,-2+a,-1+a,0+a,1+a,2+a,3+a,\cdots$$

也都是有理数,这些有理数构成的集合是$\langle I;+\rangle$的一个右陪集

$$I+a=\{i+a|i\in I\}$$

于是,子群$\langle I;+\rangle$的所有右陪集由与区间$[0,1)$中的每一个有理数a相关的右陪集组成.注意到当$a=0$时,$I+a=I$也是子群$\langle I;+\rangle$的一个右陪集.上述这些右陪集构成Q的与子群$\langle I;+\rangle$相关的右陪集分划

$$\Pi=\{I+a|0\leqslant a<1\}.$$

由于运算+可交换,对于任意$a\in Q$,$I+a=a+I$,所以这个分划简称为与$\langle I;+\rangle$相关的陪集分划.

17. 拉格朗日定理

若$\langle H;*\rangle$是群$\langle G;*\rangle$的子群,那么$\langle H;*\rangle$的所有相异左陪集的个数与$\langle H;*\rangle$的所有相异右陪集的个数相等.或者同为n个,或者都为无限个.我们称子群$\langle H;*\rangle$在群$\langle G;*\rangle$中的所有相异右(左)陪集的个数为$\langle H;*\rangle$在$\langle G;*\rangle$中的指数.

拉格朗日定理 设$\langle H;*\rangle$是有限群$\langle G;*\rangle$的子群,$\langle H;*\rangle$

在$\langle G;*\rangle$中的指数为d，则$\#G=d\cdot(\#H)$.

根据拉格朗日定理，有限群$\langle G;*\rangle$的任一子群的阶必是群$\langle G;*\rangle$的阶的因子.

例如，仔细观察例5-23的群$\langle Z_6;\oplus_6\rangle$和例5-24的群$\langle\{1,\alpha,\beta,\gamma,\delta,\varepsilon\};\circ\rangle$，它们均不可能有阶为4或阶为5的子群.

5.3 问答与论证

例5-29 设$\langle S;\circ\rangle$是一个有单位元e的半群，令

$$G=S^S=\{f\mid f:S\to S\}.$$

对任意的$f,g\in G$，任意的$x\in S$，定义$(f*g)(x)=f(x)\circ g(x)$，试证明G相对于运算$*$也构成一个有单位元的半群.

证 因为$\circ$在S上是封闭的，所以对于任意的$f,g\in G$，有$f*g\in G$，因此$\langle G;*\rangle$是一个代数系统.

对于任意的$f,g,h\in G$和任意的$x\in S$，因为S上的运算$\circ$是可结合的，故有

$$\begin{aligned}((f*g)*h)(x)&=(f*g)(x)\circ h(x)=(f(x)\circ g(x))\circ h(x)\\&=f(x)\circ(g(x)\circ h(x))=f(x)\circ(g*h)(x)\\&=(f*(g*h))(x).\end{aligned}$$

因此 $(f*g)*h=f*(g*h)$，即$*$是可结合的，故$\langle G;*\rangle$是一个半群.

定义$f_0:S\to S$，对于任意$x\in S$，$f_0(x)=e$. 于是对于任意$f\in G$和任意$x\in S$，有

$$(f*f_0)(x)=f(x)\circ f_0(x)=f(x)\circ e=f(x).$$

类似地有$(f_0*f)(x)=f(x)$. 因此f_0是$\langle G;*\rangle$中的单位元.

由上证得$\langle G;*\rangle$是一个有单位元的半群.

例5-30 设$\langle S;*\rangle$是一半群，令$G=S^S$(S^S的意义同例5-29). 函数的复合运算$\circ$在G上显然是封闭的，且因为函数的复合运算满足结合律，所以$\langle G;\circ\rangle$是一个半群. 现令G的子集

$$H = \{f_a | a \in S \text{ 且 } f_a(x) = a * x\}.$$

试证明 H 相对于运算 $\circ$ 构成 $\langle G; \circ \rangle$ 的子半群.

分析 根据子半群的定义，只要证明运算 $\circ$ 在 H 上封闭即可.

证 对于任意的 $f_a, f_b \in H$ 和任意的 $x \in S$,

$$(f_a \circ f_b)(x) = f_a(f_b(x)) = f_a(b * x) = a * (b * x)$$
$$= (a * b) * x.$$

因为 $\langle S; * \rangle$ 是半群，所以 $a * b \in S$，因此 $(f_a \circ f_b) = f_{a*b} \in H$. 故 $\circ$ 在 H 上是封闭的，$\langle H; \circ \rangle$ 是 $\langle G; \circ \rangle$ 的子半群.

例 5-31 设 $\langle S; * \rangle$ 是一个半群，且对于任意的 $a, b \in S$，由 $a \neq b$ 必有 $a * b \neq b * a$. 试证明：

(1) 对任意的 $a \in S$，有 $a * a = a$；

(2) 对任意的 $a, b \in S$，有 $a * b * a = a$；

(3) 对任意的 $a, b, c \in S$，有 $a * b * c = a * c$.

证 "由 $a \neq b$ 必有 $a * b \neq b * a$"之条件等价于"由 $a * b = b * a$ 必有 $a = b$". 我们根据与之等价的后一条件来证明.

(1) 因为运算 $*$ 是可结合的，所以对于任意 $a \in S$，有 $(a * a) * a = a * (a * a)$. 于是，根据题设条件必有 $a * a = a$.

(2) 对任意的 $a, b \in S$，有

$$(a * b * a) * a = (a * b) * (a * a) = a * b * a;$$
$$a * (a * b * a) = (a * a) * (b * a) = a * b * a;$$

因此 $$(a * b * a) * a = a * (a * b * a),$$

故 $$a * b * a = a.$$

(3) 对任意的 $a, b, c \in S$，有

$$(a * b * c) * (a * c) = (a * b) * (c * a * c) = a * b * c;$$
$$(a * c) * (a * b * c) = (a * c * a) * (b * c) = a * b * c;$$

因此 $$(a * b * c) * (a * c) = (a * c) * (a * b * c),$$

故 $$a * b * c = a * c.$$

例 5-32 试证明在一个独异点中，所有左可逆元的集合形成

一个子独异点.

说明 设$\langle S; *\rangle$是一代数系统，其中$*$是二元运算，对于元素$a\in S$，若在S中存在某个元素b，使得$b*a=e$，则称a是左可逆元，称b是a的左逆元. 此时，$a*b=e$不一定能成立，且元素a不一定存在右逆元，即此时a不一定是右可逆元.

证 设H是独异点$\langle S; *\rangle$中所有左可逆元的集合，e是$\langle S; *\rangle$的单位元. 因为$e*e=e$，所以e是左可逆元，故$e\in H$且H非空.

设$a,b\in H$，则必存在元素$a_l^{-1},b_l^{-1}\in S$，使得

$$a_l^{-1}*a=e, b_l^{-1}*b=e,$$

于是

$$(b_l^{-1}*a_l^{-1})*(a*b)=b_l^{-1}*(a_l^{-1}*a)*b=b_l^{-1}*b=e$$

因此元素$a*b$也存在左逆元$b_l^{-1}*a_l^{-1}$，有$a*b\in H$. 故$\langle H; *\rangle$是$\langle S; *\rangle$的子独异点.

例 5-33 设$\langle S; *\rangle$是一独异点，H是S中所有可逆元素的集合. 试证明$\langle H; *\rangle$是一个群.

证 显然单位元e是可逆元，所以$e\in H$，H非空.

若$a,b\in H$，则存在$a^{-1},b^{-1}\in S$，使得

$$a^{-1}*a=a*a^{-1}=e, b^{-1}*b=b*b^{-1}=e,$$

于是

$$(b^{-1}*a^{-1})*(a*b)=(a*b)*(b^{-1}*a^{-1})=e,$$

因此$a*b$也是可逆元，故$a*b\in H$，$\langle H; *\rangle$是一代数系统.

因为H是S的子集，所以运算$*$在H上也是可结合的，e也是$\langle H; *\rangle$的单位元.

对于任意$a\in H$，因为必有$a^{-1}\in S$，使$a^{-1}*a=a*a^{-1}=e$，所以a是a^{-1}的逆元，因此$a^{-1}\in H$.

由上证得，$\langle H; *\rangle$是一个群.

例 5-34 试证明凡阶分别为 1,2,3,4 的群都是交换群，举一个阶为 6 且不可交换的群的例子.

证 若$\langle G;*\rangle$是阶为 1 的群，则 G 中只有单位元 e 这唯一个元素，$e*e=e$. 显然$\langle G;*\rangle$是一交换群.

若$\langle G;*\rangle$阶为 2，设 $G=\{e,a\}$，因为 $e*e=e$，由逆元的唯一性，必有 $a*a=e$，又由 e 是单位元，有 $a*e=e*a=a$，因此$\langle G;*\rangle$是交换群. 这种群的运算表如表 5-4 所示.

表 5-4

e	e	a
e	e	a
a	a	e

若$\langle G;*\rangle$阶为 3，设 $G=\{e,a,b\}$，则因为 $e*b=b$，由群的消去律，$a*b\neq b$；因为 $a*e=a$，由群的消去律，$a*b\neq a$；因此 $a*b=e$. 于是有

$$b*a=b*a*b*b^{-1}=b*(a*b)*b^{-1}=b*e*b^{-1}=e$$

因此 $a*b=b*a$. 故$\langle G;*\rangle$是一交换群

这种群的运算表如表 5-5 所示.

表 5-5

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

由于 $a*e=a$，$a*b=e$，由群的消去律，$a*a$ 必等于 b. 类似地，$b*b$ 只能等于 a.

若$\langle G;*\rangle$阶为 4，设 $G=\{e,a,b,c\}$，下面分两种情形讨论：

(1) 若 a、b、c 中有两个元素互为逆元. 不妨设 $a*b=b*a=e$，于是 $c*c=e$. 又由 $e*c=c$，$a*e=a$，根据消去律，只能 $a*c=b$. 又因为 $e*a=a$，$c*e=c$，$b*a=e$，所以只能是 $c*a=b$. 因此 $a*c=c*a$.

类似地，因为 $e*c=c$，$b*e=b$，$b*a=e$，所以只能是 $b*c=a$. 因为 $c*e=c$，$e*b=b$，$a*b=e$，所以只能是 $c*b=a$. 因此 $b*c=c*b$.

由上可知，$\langle G;*\rangle$是一交换群. 这种群的运算表如表 5-6 所

示.

表 5-6

*	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

(2) 若 a,b,c 中每一元素都以自身为逆元. 即若 $a*a=e,b*b=e,c*c=e$,则由

$$a*e=a,e*b=b,b*b=e,\text{得 } a*b=c;$$

由 $$e*a=a,a*a=e,b*e=b,\text{得 } b*a=c;$$

因此 $$a*b=b*a.$$

类似地,可以证明 $b*c=c*b=a;a*c=c*a=b$. 因此$\langle G;*\rangle$是一交换群. 这种群的运算表如表 5-7 所示.

表 5-7

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

例 5-24 中集合 $A=\{a,b,c\}$上所有置换构成的三次对称群$\langle P;\circ\rangle$是一个阶为 6 的非交换群.

例 5-35 设$\langle G;\circ\rangle$是一个群,$u\in G$,在 G 中定义新的运算 $*$,使得对于任意的 $a,b\in G$,$a*b=a\circ u^{-1}\circ b$. 试证明$\langle G;*\rangle$也是一个群.

证 因为$\langle G;\circ\rangle$是一个群,所以运算 $*$ 在 G 上封闭.

对于任意的 $a,b,c\in G$,有

$$\begin{aligned}(a*b)*c&=(a\circ u^{-1}\circ b)*c=(a\circ u^{-1}\circ b)\circ u^{-1}\circ c\\&=a\circ u^{-1}\circ(b\circ u^{-1}\circ c)=a*(b*c),\end{aligned}$$

所以运算 $*$ 可结合.

设 $\langle G;\circ\rangle$ 的单位元为 e，则对于任意的 $a\in G$，

$$a*u=a\circ u^{-1}\circ u=a\circ e=a;$$

$$u*a=u\circ u^{-1}\circ a=e\circ a=a,$$

所以运算 $*$ 有单位元 u.

对于任意的 $a\in G$，设 a 关于运算 $\circ$ 的逆元是 a^{-1}，则 $a*(u\circ a^{-1}\circ u)=a\circ u^{-1}\circ u\circ a^{-1}\circ u=u$；

$$(u\circ a^{-1}\circ u)*a=u\circ a^{-1}\circ u\circ u^{-1}\circ a=u,$$

所以每一元素 a 关于运算 $*$ 有逆元 $u\circ a^{-1}\circ u$.

由上证得 $\langle G;*\rangle$ 是一个群.

例 5-36 试证明阶为素数的群一定是循环群.

分析 根据循环群的定义，证明此题的关键是找出生成元. 为此要尽量利用群的性质，特别是与元素周期有关的性质. 另外还要注意到题设中阶为素数的这一特点.

证 设群 $\langle G;*\rangle$ 的阶为素数 p，$G=\{e,a_1,a_2,\cdots,a_{p-1}\}$. 于是群中元素的周期只可能是 1 或 p，然而除单位元 e 的周期为 1 外，其它元素的周期均为 p. 因此，对任一 $a_i\in G$，有 $a_i^p=e$，而 $a_i^q\neq e(1\leqslant q<p)$. 令 $H=\{e,a_i,a_i^2,a_i^3,\cdots,a_i^{p-1}\}$，显然 $H\subseteq G$，且对于运算 $*$ 是封闭的，所以 $\langle H;*\rangle$ 是 $\langle G;*\rangle$ 的子群.

对于任意 $a_i^k,a_i^t\in H$，若 $a_i^k=a_i^t$（设 $k<t$），则 $a_i^k*e=a_i^k*a_i^{t-k}$，由消去律 $a_i^{t-k}=e$，而 $0<t-k<p$，这与 a_i 的周期为 p 相矛盾，因此 H 中 p 个元素互不相同，于是 $H=G$. 故 $\langle G;*\rangle$ 是一循环群. 任一元素 $a_i(1\leqslant i\leqslant p-1)$ 均是该循环群的生成元.

例 5-37 试证明循环群的子群也是循环群.

分析 证明此题的关键是找到子群的生成元.

证 设 $\langle G;*\rangle$ 是由 g 生成的循环群. $\langle H;*\rangle$ 是 $\langle G;*\rangle$ 的子群，若 $\langle H;*\rangle=\langle\{e\};*\rangle$，则显然 $\langle H;*\rangle$ 是循环群；若 $\langle H;*\rangle$ 不是单位元群，则由 $g^n\in H(n\neq 0)$，必有 $(g^n)^{-1}=g^{-n}\in H$，因此 H 中必有 g 的正指数幂. 设 r 是使得 $g^r\in H$ 的最小正整数.

对于任一$g^s \in H$，令$s=mr+i(0\leqslant i<r)$，则

$$g^i = g^{s-mr} = g^s * (g^r)^{-m} \in H$$

但由r是最小正整数之假设，必有$i=0$. 于是$s=mr$，即$g^s=(g^r)^m$，故$\langle H; * \rangle$是由g^r生成的循环群.

例 5-38 设$\langle G; * \rangle$是一循环群，f是从$\langle G; * \rangle$到$\langle G'; \circ \rangle$的满同态($\circ$是二元运算). 试证明$\langle G'; \circ \rangle$也是循环群.

证 因为f是从群$\langle G; * \rangle$到$\langle G'; \circ \rangle$的满同态，由满同态的性质，$\langle G'; \circ \rangle$也是一个群.

设g是群$\langle G; * \rangle$的生成元，且$f(g)=g'$. 对任一$a' \in G'$，由f是满射，必存在$a\in G$，使得$f(a)=a'$. 设$a=g^i$(i为某一整数)，则

$$a' = f(a) = f(g^i).$$

若$i=0$，则$a'=f(g^0)=f(e)=e'=(g')^0$；

若$i>0$，则$a'=f(g^i)=f\underbrace{(g*g*\cdots*g)}_{i个}=\underbrace{f(g)\circ f(g)\circ\cdots\circ f(g)}_{i个}=(g')^i$.

若$i<0$，则$i=-|i|$，于是由满同态的性质，

$$a' = f(g^i) = f((g^{|i|})^{-1}) = (f(g^{|i|}))^{-1}$$
$$= ((g')^{|i|})^{-1} = (g')^i.$$

由$a' \in G'$的任意性，$\langle G'; \circ \rangle$是一循环群.

例 5-39 设$\langle A; * \rangle$和$\langle B; * \rangle$都是群$\langle G; * \rangle$的子群，令G的子集

$$A*B = \{a*b|a \in A, b \in B\},$$

试问$A*B$能否成为$\langle G; * \rangle$的子群.

解 $A*B$不一定能成为$\langle G; * \rangle$的子群. 例如在例 5-24 中$\langle\{1,\alpha\}; \circ\rangle$和$\langle\{1,\beta\}; \circ\rangle$均是群$\langle P; \circ \rangle$的子群，但$\{1,\alpha\}\circ\{1,\beta\}=\{1,\alpha,\beta,\gamma\}$对于运算$\circ$不封闭，因而不能构成$\langle P; \circ \rangle$的子群.

但也有可能$A*B$能成为$\langle G; * \rangle$的子群. 例如，若在例 5-24

中 $A=\{1,\alpha\}$, $B=\{1,\gamma,\delta\}$，则

$$\{1,\alpha\}\circ\{1,\nu,\delta\}=\{1,\nu,\delta,\alpha,\beta,\varepsilon\}=P.$$

因此 $\{1,\alpha\}\circ\{1,\nu,\delta\}$ 能成为 $\langle G;*\rangle$ 的子群.

例 5-40 设 $\langle A;*\rangle$ 和 $\langle B;*\rangle$ 都是群 $\langle G;*\rangle$ 的正规子群. 试证明 $A*B$ 对于运算 $*$ 也构成 $\langle G;*\rangle$ 的正规子群.

分析 ① $\langle A;*\rangle$ 是 $\langle G;*\rangle$ 的正规子群意味着对于任意的 $g\in G$, $g*A=A*g$. 同样地，$\langle B;*\rangle$ 是 $\langle G;*\rangle$ 的正规子群意味着对于任意的 $g\in G$, $g*B=B*g$.

② $g*A=A*g$ 意味着对于任意的 $a\in A$，必存在元素 $a'\in A$，使得 $g*a=a'*g$. 特别要注意的是，这里不能写作 $g*a=a*g$.

③要证明 $A*B$ 与运算 $*$ 能构成 $\langle G;*\rangle$ 的正规子群，需要证明以下两点：

1）$A*B$ 与运算 $*$ 能构成 $\langle G;*\rangle$ 的子群：由 $a_1*b_1, a_2*b_2\in A*B$，可推出 $(a_1*b_1)*(a_2*b_2)^{-1}\in A*B$；

2）$\langle A*B;*\rangle$ 是 $\langle G;*\rangle$ 的正规子群：对于任意 $g\in G$, $g*(A*B)*g^{-1}\subseteq A*B$. 即对于任意的 $g\in G$ 和任意的 $a*b\in A*B$, $g*(a*b)*g^{-1}\in A*B$.

证 因为 $e\in A, e\in B$，所以 $e\in A*B$，因此 $A*B$ 非空.

对于任意的 $a_1*b_1, a_2*b_2\in A*B$，因为 $\langle A;*\rangle$ 是 $\langle G;*\rangle$ 的正规子群，所以

$$\begin{aligned}(a_1*b_1)*(a_2*b_2)^{-1}&=(a_1*b_1)*(b_2^{-1}*a_2^{-1})\\&=a_1*(b_1*b_2^{-1})*a_2^{-1}=a_1*(b_3*a_2^{-1})\\&=a_1*(a_3*b_3)=(a_1*a_3)*b_3\in A*B.\end{aligned}$$

由上式知 $\langle A*B;*\rangle$ 是群 $\langle G;*\rangle$ 的子群.

对于任意的 $g\in G$ 和任意的 $a*b\in A*B$，因为 $\langle B;*\rangle$ 也是 $\langle G;*\rangle$ 的正规子群，所以

$$\begin{aligned}g*(a*b)*g^{-1}&=(g*a)*(b*g^{-1})=(a'*g)*(g^{-1}*b')\\&=a'*(g*g^{-1})*b'=a'*b'\in A*B.\end{aligned}$$

这说明对于任意的 $g\in G, g*(A*B)*g^{-1}\subseteq A*B$,故 $\langle A*B;*\rangle$ 是 $\langle G;*\rangle$ 的正规子群.

例 5-41 设 $\langle A;*\rangle$ 和 $\langle B;*\rangle$ 都是群 $\langle G;*\rangle$ 的子群. 试证明 $\langle A*B;*\rangle$ 是 $\langle G;*\rangle$ 的子群的充要条件是 $A*B=B*A$.

证 充分性

因为 $e\in A, e\in B$,所以 $e\in A*B$,因此 $A*B$ 非空.

对于任意的 $a_1*b_1, a_2*b_2\in A*B$,因为 $\langle A;*\rangle$ 和 $\langle B;*\rangle$ 都是 $\langle G;*\rangle$ 的子群,所以

$$
\begin{aligned}
(a_1*b_1)*(a_2*b_2)^{-1} &= (a_1*b_1)*(b_2^{-1}*a_2^{-1}) \\
&= a_1*(b_1*b_2^{-1})*a_2^{-1} = a_1*(b_3*a_2^{-1}) \\
&\quad (b_3\in B, a_2^{-1}\in A).
\end{aligned}
$$

因为 $A*B=B*A$,所以必有 $a_3\in A, b_4\in B$,使得

$$b_3*a_2^{-1}=a_3*b_4, \text{于是}$$

$$(a_1*b_1)*(a_2*b_2)^{-1}=a_1*(a_3*b_4)=(a_1*a_3)*b_4\in A*B.$$

由此可知 $\langle A*B;*\rangle$ 是 $\langle G;*\rangle$ 的子群.

必要性 设 $b*a\in B*A$,则有 $b^{-1}\in B, a^{-1}\in A$,所以 $a^{-1}*b^{-1}\in A*B$. 因为 $\langle A*B;*\rangle$ 是 $\langle G;*\rangle$ 的子群,所以又有 $(a^{-1}*b^{-1})^{-1}\in A*B$,即 $b*a\in A*B$,因此 $B*A\subseteq A*B$.

设 $a*b\in A*B$,则由 $\langle A*B;*\rangle$ 是 $\langle G;*\rangle$ 的子群,必有元素 $a_1*b_1\in A*B$,使得 $a*b=(a_1*b_1)^{-1}$,即 $a*b=b_1^{-1}*a_1^{-1}$,而 $b_1^{-1}*a_1^{-1}\in B*A$,所以 $a*b\in B*A$,因此 $A*B\subseteq B*A$.

由上证得 $A*B=B*A$.

例 5-42 设 $\langle G;*\rangle$ 是一个群,H 是 G 的非空子集. 试证明 $\langle H;*\rangle$ 是 $\langle G;*\rangle$ 的子群的充要条件 $\langle H;*\rangle$ 是一个群.

证 充分性 设 $\langle H;*\rangle$ 是群,则显然 $\langle H;*\rangle$ 是 $\langle G;*\rangle$ 的子代数. 设 e' 是 $\langle H;*\rangle$ 的单位元,则有 $e'*e'=e'$. 由 e 是群 $\langle G;*\rangle$ 的单位元,有 $e*e'=e'$. 于是 $e'*e'=e*e'$. 由消去律 $e'=e$. 因此 $e\in H$.

对任意 $a\in H$,设 a' 是 a 在群 $\langle H;*\rangle$ 中的逆元,于是有 $a*a'$

$=e$. 另一方面 $a*a^{-1}=e$. 由消去律 $a'=a^{-1}$. 因此 $a^{-1}\in H$. 由此证得，$\langle H;*\rangle$是$\langle G;*\rangle$的子群.

必要性 设$\langle H;*\rangle$是$\langle G;*\rangle$的子群，则显然$\langle H;*\rangle$是一代数系统，且运算 $*$ 在 H 上可结合. 单位元 $e\in H$，显然 e 也是$\langle H;*\rangle$中的单位元，对于任一 $a\in H$，有 $a^{-1}\in H$，满足 $a*a^{-1}=a^{-1}*a=e$. 因此$\langle H;*\rangle$是一个群.

例 5-43 设$\langle G;*\rangle$是一个群，$\langle \widetilde{G};*\rangle$是$\langle G;*\rangle$的一个子群，定义 G 的子集

$$H=\{a\mid a*\widetilde{G}=\widetilde{G}*a\}.$$

试证明(1) $\langle H;*\rangle$是$\langle G;*\rangle$的子群；

(2) $\langle \widetilde{G};*\rangle$是$\langle H;*\rangle$的正规子群.

证明此题之前，我们证明如下结论：在一个群中，元素与子集的运算也是满足结合律的.

设$\langle G;*\rangle$是一个群，$\widetilde{G}\subseteq G$，于是对于任意的 $a,b\in G$，

$$(a*b)*\widetilde{G}=\{(a*b)*g\mid g\in\widetilde{G}\}.$$

因为$(a*b)*g=a*(b*g)$，所以

$$\begin{aligned}(a*b)*\widetilde{G}&=\{a*(b*g)\mid g\in\widetilde{G}\}\\&=\{a*(b*g)\mid b*g\in b*\widetilde{G}\}=a*(b*\widetilde{G}).\end{aligned}$$

类似地也可证明 $\widetilde{G}*(a*b)=(\widetilde{G}*a)*b$，$(a*\widetilde{G})*b=a*(\widetilde{G}*b)$.

证 (1) 显然 $e*\widetilde{G}=\widetilde{G}*e$，所以 $e\in H$，H 非空.

设 $a,b\in H$，则 $a*\widetilde{G}=\widetilde{G}*a$，$b*\widetilde{G}=\widetilde{G}*b$，于是

$$\begin{aligned}(a*b)*\widetilde{G}&=a*(b*\widetilde{G})=a*(\widetilde{G}*b)=(a*\widetilde{G})*b\\&=(\widetilde{G}*a)*b=\widetilde{G}*(a*b).\end{aligned}$$

因此 $a*b\in H$.

设 $a\in H$，则

$$\begin{aligned}a^{-1}*\widetilde{G}&=(a^{-1}*\widetilde{G})*(a*a^{-1})=a^{-1}*(\widetilde{G}*a)*a^{-1}\\&=a^{-1}*(a*\widetilde{G})*a^{-1}\\&=(a^{-1}*a)*\widetilde{G}*a^{-1}=\widetilde{G}*a^{-1},\end{aligned}$$

因此 $a^{-1}\in H$.

由上证得，$\langle H;*\rangle$ 是 $\langle G;*\rangle$ 的子群.

(2) 因为 $e*\widetilde{G}=\widetilde{G}*e=\widetilde{G}$，所以 $\widetilde{G}$ 是 $\langle \widetilde{G};*\rangle$ 的一个左陪集，也是一个右陪集. 于是，对于任意的 $a\in\widetilde{G}$，

$$a*\widetilde{G}=e*\widetilde{G}=\widetilde{G}*e=\widetilde{G}*a,$$

因此 $\widetilde{G}\subseteq H$.

因为 $\langle\widetilde{G};*\rangle$ 是 $\langle G;*\rangle$ 的子群，由例 5-42 $\langle\widetilde{G};*\rangle$ 是一个群. 又由 $\langle H;*\rangle$ 是群且 $\widetilde{G}\subseteq H$，所以 $\langle\widetilde{G};*\rangle$ 必是 $\langle H;*\rangle$ 的子群.

由 H 的定义，对于任意 $a\in H$，都有 $a*\widetilde{G}=\widetilde{G}*a$，因此 $\langle\widetilde{G};*\rangle$ 是 $\langle H;*\rangle$ 的正规子群.

例 5-44 试证明：如果群 $\langle G;*\rangle$ 的每一个元素都是它自己的逆元，则该群必是交换群.

证 因为对于任意 $a,b\in G$，有 $a^2=e$，$b^2=e$ 且 $(a*b)^2=e$，所以 $(a*b)^2=a^2*b^2$. 根据例 5-10，$\langle G;*\rangle$ 必是交换群.

例 5-45 设 g 是由群 $\langle G;*\rangle$ 到群 $\langle G';\circ\rangle$ 的满同态，试证明：

(1) 若 $\langle H;*\rangle$ 是群 $\langle G;*\rangle$ 的子群，则 H 的象 H' 对于运算 $\circ$ 也构成 $\langle G';\circ\rangle$ 的子群；

(2) 若 $\langle N;*\rangle$ 是群 $\langle G;*\rangle$ 的正规子群，则 N 的象 N' 对于运算 $\circ$ 也构成 $\langle G';\circ\rangle$ 的正规子群.

证 (1) 由 $e\in H$，则 $g(e)=e'\in H'$. 因此 H' 非空.

对于任意的 $a',b'\in H'$，因为 H' 是 H 的象，所以必存在 $a,b\in H$，使 $g(a)=a'$，$g(b)=b'$，又由 g 是满同态，因此

$$\begin{aligned} a'\circ(b')^{-1} &= g(a)\circ(g(b))^{-1} \\ &= g(a)\circ g(b^{-1}) = g(a*b^{-1}). \end{aligned}$$

由于 $\langle H;*\rangle$ 是 $\langle G;*\rangle$ 的子群，因此由 $a,b\in H$ 可知 $a*b^{-1}\in H$，于是 $a'\circ(b')^{-1}\in H'$. 故 $\langle H';\circ\rangle$ 是群 $\langle G';\circ\rangle$ 的子群.

(2) 若 $\langle N;*\rangle$ 是群 $\langle G;*\rangle$ 的正规子群，则由 (1) 知 $\langle N';\circ\rangle$ 是群 $\langle G';\circ\rangle$ 的子群.

对于任意的 $a'\in G'$ 和任意的 $n'\in N'$，必有 $a\in G$ 和 $n\in N$，

使得 $g(a)=a'$，$g(n)=n'$，因此

$$a' \circ n' \circ (a')^{-1} = g(a) \circ g(n) \circ (g(a))^{-1} = g(a) \circ g(n) \circ g(a^{-1})$$
$$= g(a * n * a^{-1}).$$

因为 $\langle N; * \rangle$ 是 $\langle G; * \rangle$ 的正规子群，所以 $a * N * a^{-1} \subseteq N$. 因此 $a * n * a^{-1} \in N$. 于是 $a' \circ n' \circ (a')^{-1} \in N'$.

由 $a' \in G'$ 和 $n' \in N'$ 的任意性知，对任意的 $a' \in G'$，有 $a' \circ N' \circ (a')^{-1} \subseteq N'$. 故 $\langle N'; \circ \rangle$ 是 $\langle G'; \circ \rangle$ 的正规子群.

例 5-46 试证明所有无限阶的循环群都相互同构. 又凡阶等于 n 的有限循环群也都相互同构.

分析 证明本题时注意循环群有如下的性质：设 $\langle G; * \rangle$ 是一由元素 g 生成的循环群，(1) 若 g 的周期为 n，则 $\langle G; * \rangle$ 是一个 n 阶的有限循环群；(2) 若 g 的周期为无限，则 $\langle G; * \rangle$ 是一个无限阶的循环群. 这条性质说明，循环群 $\langle G; * \rangle$ 的阶与其生成元的周期是相同的（可参阅[1]的定理 5-5).

证 设 $\langle G_1; * \rangle$ 和 $\langle G_2; \circ \rangle$ 是两个无限阶的循环群，g_1 和 g_2 分别是它们的生成元.

定义函数 $f: G_1 \to G_2$，使得对于任意 $g_1^i \in G_1$，$f(g_1^i)=g_2^i$. 对于任意 $b \in G_2$，必存在整数 i，使得 $b=g_2^i$，由 f 的定义，$f(g_1^i)=g_2^i=b$，$g_1^i \in G_1$，所以 f 是满射.

又对于任意 $a_1, a_2 \in G_1$，必存在整数 j, k，使得 $a_1=g_1^j$，$a_2=g_1^k$，于是

$$b_1 = f(a_1) = f(g_1^j) = g_2^j, b_2 = f(a_2) = f(g_1^k) = g_2^k.$$

设 $a_1 \neq a_2$，则 $j \neq k$，(反证法)如果 $b_1=b_2$，即 $g_2^j=g_2^k$(设 $j<k$)，则 $g_2^j = g_2^{k-j} \circ g_2^j$，于是 $g_2^{k-j}=e$，而 $k-j>0$，这与 g_2 具有无限周期相矛盾. 因此 $b_1 \neq b_2$. 故 f 是内射. 因此 f 是双射.

对于任意 $g_1^i, g_1^j \in G_1$，

$$f(g_1^i * g_1^j) = f(g_1^{i+j}) = g_2^{i+j};$$
$$f(g_1^i) \circ f(g_1^j) = g_2^i \circ g_2^j = g_2^{i+j};$$

因此
$$f(g_1^i * g_1^j) = f(g_1^i) \circ f(g_1^j).$$

故 f 是由$\langle G_1;*\rangle$到$\langle G_2;\circ\rangle$的同构.

设$\langle G_1;*\rangle$和$\langle G_2;\circ\rangle$是两个 n 阶的有限循环群，g_1 和 g_2 分别是它们的生成元. 于是 $g_1^n=e_1$，$g_2^n=e_2$，并可令

$$G_1=\{g_1,g_1^2,\cdots,g_1^{n-1},g_1^n\},G_2=\{g_2,g_2^2,\cdots,g_2^{n-1},g_2^n\}.$$

定义函数 $f:G_1\rightarrow G_2$，使得对于任意 $g_1^i\in G_1$，$f(g_1^i)=g_2^i$. 显然 f 是一个双射.

关于 f 满足同态条件的证明，与群是无限阶的情形时完全相同，此处不再重复.

读者要清楚的是，对于任意整数 i，均有 $g_1^i\in G_1$，$g_2^i\in G_2$. 当 $i\notin\{1,2,\cdots,n-1,n\}$时，$g_1^i$ 必与 G_1 中某一元素相同. 类似地，g_2^i 也必与 G_2 中某一元素相同.

第六章　环和域

6.1　内容提要

1. 环

2. 子环

3. 域

6.2　基本知识点

1. 环

环是具有两个二元运算的代数系统〈R；＋，∘〉，它必须满足以下三个条件：

(1)〈R；＋〉是一个交换群；

(2)〈R；·〉是半群；

(3)运算·对＋是可分配的.

在上述环的定义中，R 表示一个任意的非空集合. 我们常将环〈R；＋，·〉中的运算＋称为加法，将运算·称为乘法，用 $-a$ 表示 a 的加法逆元.

例 6-1　设 R 是实数集，加法＋是通常数的加法，但乘法×是 $a\times b=|a|\cdot b$，问〈R；＋，×〉是否构成环?

解　显然，实数集 R 对于通常数的加法运算构成交换群〈R；

$+\rangle$.

对于任意的 $a,b,c\in R$，有

$a\times(b\times c)=a\times(|b|\cdot c)=|a|\cdot(|b|\cdot c)=|a|\cdot|b|\cdot c$,

$(a\times b)\times c=(|a|\cdot b)\times c=||a|\cdot b|\cdot c=|a|\cdot|b|\cdot c$,

即 $a\times(b\times c)=(a\times b)\times c$. 故$\langle R;\times\rangle$是半群.

对于任意的 $a,b,c\in R$，有

$$a\times(b+c)=|a|\cdot(b+c)=|a|\cdot b+|a|\cdot c;$$

$$a\times b+a\times c=|a|\cdot b+|a|\cdot c;$$

即 $$a\times(b+c)=a\times b+a\times c,$$

但是 $$(b+c)\times a=|b+c|\cdot a,$$

$$b\times a+c\times a=|b|\cdot a+|c|\cdot a.$$

由于一般情形下 $|b+c|\cdot a\neq|b|\cdot a+|c|\cdot a$，所以$\times$对加的分配律不成立. 故$\langle R;+,\times\rangle$不能构成环.

例如， $|-5+2|\cdot 3\neq|-5|\cdot 3+|2|\cdot 3$.

例6-2 证明$\langle I;\oplus,\odot\rangle$是一个环. 这里 I 表示整数集，运算$\oplus$和$\odot$的定义如下：

$$a\oplus b=a+b-1, a\odot b=a+b-ab.$$

证 对于任意的 $a,b,c\in I$，

$$(a\oplus b)\oplus c=(a+b-1)\oplus c=a+b-1+c-1$$
$$=a+b+c-2,$$
$$a\oplus(b\oplus c)=a\oplus(b+c-1)=a+b+c-1-1$$
$$=a+b+c-2,$$

所以$(a\oplus b)\oplus c=a\oplus(b\oplus c)$. 运算$\oplus$显然也是可交换的.

对任意 $a\in I$，有

$$1\oplus a=1+a-1=a, a\oplus 1=a+1-1=a,$$

所以 1 是运算$\oplus$的单位元.

对于任意的 $a\in I$, $2-a\in I$ 且

$$a\oplus(2-a)=(2-a)\oplus a=a+2-a-1=1,$$

所以 $2-a$ 是 a 的逆元.

由上证得$\langle R;\oplus\rangle$是一交换群.

对于任意的$a,b,c\in I$,有

$$\begin{aligned}
a\odot(b\odot c) &= a\odot(b+c-bc) = a+b+c-bc \\
&\quad -a(b+c-bc) \\
&= a+b+c-bc-ab-ac+abc, \\
(a\odot b)\odot c &= (a+b-ab)\odot c \\
&= a+b-ab+c-(a+b-ab)c \\
&= a+b+c-ab-ac-bc+abc,
\end{aligned}$$

所以运算$\odot$是可结合的. 因此$\langle R;\odot\rangle$是一个半群.

对于任意的$a,b,c\in I$,有

$$\begin{aligned}
a\odot(b\oplus c) &= a\odot(b+c-1) = a+(b+c-1) \\
&\quad -a(b+c-1) = 2a+b+c-ab-ac-1, \\
(a\odot b)\oplus(a\odot c) &= (a+b-ab)\oplus(a+c-ac) \\
&= 2a+b+c-ab-ac-1,
\end{aligned}$$

所以

$$a\odot(b\oplus c) = (a\odot b)\oplus(a\odot c).$$

由于运算$\odot$可交换,所以

$$(b\oplus c)\odot a = (b\odot a)\oplus(c\odot a).$$

因此,$\odot$对$\oplus$可分配.

由上可知$\langle I;\oplus,\odot\rangle$是一个环.

2. 子环及其判别

类似于子群,环中也有子环的概念,只是定义的方式稍有不同.

设$\langle R;+,\cdot\rangle$是一个环,$\langle H;+,\cdot\rangle$是$\langle R;+,\cdot\rangle$的子代数,如果$\langle H;+,\cdot\rangle$也是一个环,则称$\langle H;+,\cdot\rangle$是$\langle R;+,\cdot\rangle$的于环.

设$\langle R;+,\cdot\rangle$是一个环,H是R的非空子集,如何判别H与运算$+,\cdot$能否构成$\langle R;+,\cdot\rangle$的子环呢? 根据子环的定义,$\langle H;$

$+,\cdot$)必须是一个环. 也就是说 H 必须满足:

(1)运算+与·在 H 上封闭:$\langle H;+,\cdot\rangle$ 成为 $\langle R;+,\cdot\rangle$ 的子代数;

(2)$\langle H;+\rangle$ 必须是一个群. 即 $\langle H;+\rangle$ 必须是 $\langle R;+\rangle$ 的子群;

(3)+在 H 上可交换;

(4)·在 H 上可结合;

(5)在 H 中·对+可分配.

然而,因为 $\langle R;+,\cdot\rangle$ 是一个环,H 是 R 的子集,所以条件(3)、(4)、(5)是自然满足的,用不着再去判别. 因此要判别 H 与+、·能否构成 $\langle R;+,\cdot\rangle$ 的子环,只要判别(1),(2)两条,具体地说,要判别:

1)封闭性:由 $a,b\in H$,推出 $a+b\in H$ 且 $a\cdot b\in H$;

2)加法的可逆性:由 $a\in H$,推出 a 的加法逆元 $-a\in H$.

例 6-3 找出环 $\langle Z_6;\oplus_6,\odot_6\rangle$ 的所有子环. 在这里 $Z_6=\{0,1,2,3,4,5\}$,$\oplus_6$ 和 $\odot_6$ 分别表示模 6 的加法和乘法,即

$$a\oplus_6 b=\mathrm{res}_6(a+b),a\odot_6 b=\mathrm{res}_6(ab).$$

解 关于 Z_6 与 $\oplus_6$、$\odot_6$ 构成环的证明我们不进行讨论. 读者可根据环的定义自己去证明. 为了后面讨论的方便,我们给出 $\oplus_6$ 与 $\odot_6$ 的运算表(表 6-1 和表 6-2).

表 6-1

$\oplus_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

表 6-2

$\odot_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

根据拉格朗日定理，若$\langle H;\oplus_6\rangle$是$\langle Z_6;\oplus_6\rangle$的子群，则$\# H$应是$\# G$的因子. 因此$\# H$只可能为1、2、3或6.

根据子群的定义，若$\langle H;\oplus_6\rangle$是$\langle Z_6;\oplus_6\rangle$的子群，则由$a\in H$，相应也有$a$的加法逆元$-a\in H$. 并且加法单位元$0\in H$.

又注意到1与5互为加法逆元，2与4互为加法逆元，3和0均以自身为逆元.

由上分析可知，H只有以下可能：$H=\{0\}$或$H=\{0,3\}$，或$H=\{0,1,5\}$，或$H=\{0,2,4\}$，或$H=Z_6$. 用条件1)、2)来判别，发现当$H=\{0,1,5\}$时，运算$\oplus_6$在H上不封闭. H的其它几种情形均满足条件1)和2)，因此环$\langle Z_6;\oplus_6,\odot_6\rangle$有如下一些子环：

$$\langle\{0\};\oplus_6,\odot_6\rangle;\langle\{0,3\};\oplus_6,\odot_6\rangle;$$
$$\langle\{0,2,4\};\oplus_6,\odot_6\rangle;\langle Z_6;\oplus_6,\odot_6\rangle.$$

在环$\langle R;+,\cdot\rangle$中我们将加法$+$的单位元用0表示，并将它称作零元素. 其原因是对于乘法$\cdot$它具有数0的性质，即对于任意$a\in R$，

$$0\cdot a=a\cdot 0=0.$$

对此可用与例4-10中完全相同的方法证明.

环的定义中并不需求$\cdot$满足交换律，如果一个环的运算$\cdot$满足交换律，则称该环为可换环.

3. 域

如果环$\langle R;+,\cdot\rangle$是一含有非零元素(即至少有两个元素)的可换环，具有乘法单位元且每个非零元素具有关于$\cdot$的逆元，则称$\langle R;+,\cdot\rangle$是一个域. 也就是说域是一种特殊的环.

例6-4 试判别$\langle Z_3;\oplus_3,\odot_3\rangle$和$\langle Z_4;\oplus_4,\odot_4\rangle$是不是域.

解 根据环的定义容易证明，对于任意正整数m，$\langle Z_m;\oplus_m,\odot_m\rangle$是一个环. 因此对于$\langle Z_3;\oplus_3,\odot_3\rangle$和$\langle Z_4;\oplus_4,\odot_4\rangle$，我们只需判别它们是否满足以下三个条件：

(1)运算$\odot_3$和$\odot_4$是否可交换；

(2)运算$\odot_3$和$\odot_4$是否具有单位元;

(3)Z_3和Z_4中的每一个非零元素分别对于$\odot_3$和$\odot_4$是否具有逆元.

为此我们构造$\odot_3$和$\odot_4$的运算表(表 6-3 和表 6-4)如下

表 6-3

$\odot_3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

表 6-4

$\odot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

从表 6-3 中我们可看出$\odot_3$是可交换的,1 是其单位元,1 的逆元$1^{-1}=1$,2 的逆元$2^{-1}=2$. 因此$\langle Z_3;\oplus_3,\odot_3\rangle$是一个域.

从表 6-4 中我们可看出$\odot_4$是可交换的,1 是其单位元,1 的逆元$1^{-1}=1$,3 的逆元$3^{-1}=3$. 但是 2 没有逆元,因此$\langle Z_4;\oplus_4,\odot_4\rangle$不是域.

比较整环与环的定义可以看出,整环也是环,但它是必须满足以下三个条件的环:

(1)乘法运算·是可交换的;

(2)·具有单位元;

(3)·满足消去律.

6.3 问答与论证

例 6-5 设$\langle R;+,\cdot\rangle$是环,又设a、b和c是R中的任意元素,试证明:

(1) $a\cdot(-b)=(-a)\cdot b=-(a\cdot b)$;

(2) 若 $a \cdot b = b \cdot a$，则 $a \cdot (-b) = (-b) \cdot a$，$a \cdot (nb) = (nb) \cdot a$（$n$ 为非负整数）以及 $a \cdot b^{-1} = b^{-1} \cdot a$；

(3) 若 $a \cdot b = b \cdot a$ 和 $a \cdot c = c \cdot a$，则 $a \cdot (b+c) = (b+c) \cdot a$，$a \cdot (b \cdot c) = (b \cdot c) \cdot a$.

说明 在环 $\langle R; +, \cdot \rangle$ 中为区别起见，对于任意 $a \in R$，我们用 $-a$ 表示 a 的加法逆元，用 a^{-1} 表示 a 的乘法逆元，用 na 表示 $\underbrace{a+a+\cdots+a}_{n个}$，用 a^n 表示 $\underbrace{a \cdot a \cdot \cdots \cdot a}_{n个}$，用 0 表示加法单位元，用 1 表示乘法单位元.

证 (1) 因为

$$a \cdot b + a \cdot (-b) = a \cdot (b + (-b)) = a \cdot 0 = 0,$$

所以

$$a \cdot (-b) = -(a \cdot b).$$

类似地 $(-a) \cdot b = -(a \cdot b)$.

(2) 因为 $a \cdot b = b \cdot a$，所以

$$a \cdot (-b) = -(a \cdot b) = -(b \cdot a) = (-b) \cdot a;$$

$$\begin{aligned} a \cdot (nb) &= a \cdot (b + b + \cdots + b) = a \cdot b + a \cdot b + \cdots + a \cdot b \\ &= b \cdot a + b \cdot a + \cdots + b \cdot a = (b + b + \cdots + b) \cdot a \\ &= (nb) \cdot a. \end{aligned}$$

题目要求证明 $a \cdot b^{-1} = b^{-1} \cdot a$，说明元素 b 存在乘法逆元，且乘法存在单位元 1. 但此时其它的元素不一定有乘法逆元.

$$\begin{aligned} a \cdot b^{-1} &= 1 \cdot (a \cdot b^{-1}) = (b^{-1} \cdot b) \cdot (a \cdot b^{-1}) = b^{-1}(b \cdot a) \cdot b^{-1} \\ &= b^{-1} \cdot (a \cdot b) \cdot b^{-1} = (b^{-1} \cdot a) \cdot (b \cdot b^{-1}) = b^{-1} \cdot a. \end{aligned}$$

(3) 因为 $a \cdot b = b \cdot a$，$a \cdot c = c \cdot a$，所以

$$a \cdot (b + c) = a \cdot b + a \cdot c = b \cdot a + c \cdot a = (b + c) \cdot a;$$

$$\begin{aligned} a \cdot (b \cdot c) &= (a \cdot b) \cdot c = (b \cdot a) \cdot c = b \cdot (a \cdot c) = b \cdot (c \cdot a) \\ &= (b \cdot c) \cdot a. \end{aligned}$$

例 6-6 设 $\langle R; +, \cdot \rangle$ 是一有乘法单位元的环，定义 R 的一个子集 H 为

$$H = \{a \mid a^{-1} \text{ 也在 } R \text{ 中}\}.$$

试证明$\langle H;\cdot\rangle$是一个群.

分析 根据群的定义，为了证明$\langle H;\cdot\rangle$是一个群，需证明以下四条：

(1)运算·在H上封闭. 因此$\langle H;\cdot\rangle$是一代数系统；

(2)运算·在H上可结合；

(3)·的单位元$1\in H$；

(4)·在H上满足可逆性：由$a\in H$，可推出$a^{-1}\in H$.

证 因为$1^{-1}=1\in R$，所以$1\in H$，且H非空.

对于任意$a,b\in H$，必有$a^{-1}\in R,b^{-1}\in R$，因此$b^{-1}\cdot a^{-1}\in R$，并且

$$(b^{-1}\cdot a^{-1})\cdot(a\cdot b)=(a\cdot b)\cdot(b^{-1}\cdot a^{-1})=1,$$

因此 $(a\cdot b)^{-1}=b^{-1}\cdot a^{-1}\in R$，于是$a\cdot b\in H$，故$\langle H;\cdot\rangle$是一代数系统.

因为H是R的子集，·在H上可结合是显然的.

对于任意$a\in H$，必有$a^{-1}\in R$，由于a与a^{-1}互为逆元，所以$(a^{-1})^{-1}=a\in R$，因此$a^{-1}\in H$.

由上证得$\langle H;\cdot\rangle$是一个群.

例 6-7 设$\langle R;+,\cdot\rangle$是环，其乘法单位元记为1，加法单位元记为0，对于任意$a,b\in R$，定义$a\oplus b=a+b+1$，$a\odot b=a\cdot b+a+b$. 试证明$\langle R;\oplus,\odot\rangle$也是环，并且与环$\langle R;+,\cdot\rangle$同构.

证 运算$\oplus$和$\odot$在R上显然是封闭的. 运算+可交换，因此$\oplus$也可交换.

对于任意的$a,b,c\in R$，

$$\begin{aligned}(a\oplus b)\oplus c&=(a+b+1)\oplus c=a+b+1+c+1\\&=a+(b+c+1)+1=a\oplus(b\oplus c).\end{aligned}$$

元素1的加法逆元记作-1，则对于任意的$a\in R$，

$$a\oplus -1=a+(-1)+1=a+0=a.$$

由$\oplus$的交换性知-1是运算$\oplus$的单位元.

对于任意$a\in R$，

$$
\begin{aligned}
a \oplus ((-a)+2(-1)) &= a \oplus ((-a)+(-1)+(-1)) \\
&= a+((-a)+(-1)+(-1))+1 \\
&= (a-(-a)) \\
&\quad +(-1)+((-1)+1) \\
&= 0+(-1)+0=-1.
\end{aligned}
$$

由$\oplus$的交换性知，$(-a)+2(-1)$是 a 的加法逆元.

由上证得$\langle R;\oplus\rangle$是一交换群.

对于任意的 $a,b,c\in R$，因为运算 · 对+是可分配的，且+是可交换的，所以

$$
\begin{aligned}
& a\odot(b\odot c) \\
&= a\cdot(b\odot c)+a+(b\odot c) \\
&= a\cdot(b\cdot c+b+c)+a+(b\cdot c+b+c) \\
&= a\cdot b\cdot c+a\cdot b+a\cdot c+b\cdot c+a+b+c;
\end{aligned}
$$

$$
\begin{aligned}
(a\odot b)\odot c &= (a\odot b)\cdot c+(a\odot b)+c \\
&= (a\cdot b+a+b)\cdot c+(a\cdot b+a+b)+c \\
&= a\cdot b\cdot c+a\cdot b+a\cdot c+b\cdot c+a+b+c,
\end{aligned}
$$

因此 $\quad a\odot(b\odot c)=(a\odot b)\odot c.$

由上证得$\langle R;\odot\rangle$是一半群.

对于任意 $a,b,c\in R$，有

$$
\begin{aligned}
a\odot(b\oplus c) &= a\cdot(b\oplus c)+a+(b\oplus c) \\
&= a\cdot(b+c+1)+a+(b+c+1);
\end{aligned}
$$

$$
\begin{aligned}
(a\odot b)\oplus(a\odot c) &= (a\cdot b+a+b)\oplus(a\cdot c+a+c) \\
&= (a\cdot b+a+b)+(a\cdot c+a+c)+1 \\
&= (a\cdot b+a\cdot c+a)+(a+b+c+1) \\
&= a(b+c+1)+a+(b+c+1),
\end{aligned}
$$

因此 $\quad a\odot(b\oplus c)=(a\odot b)\oplus(a\odot c).$

类似地可以证明 $\quad (b\oplus c)\odot a=(b\odot a)\oplus(c\odot a).$

由上可知，$\langle R;\oplus,\odot\rangle$是环.

定义函数 $f:R\to R$，使对于任意 $a\in R$，$f(a)=a+(-1)=a-$

1 （注：在环中，我们通常将 $a+(-b)$ 简写成 $a-b$.）

对于任意 $a\in R$，存在元素 $a+1\in R$，使

$$f(a+1)=(a+1)-1=a+(1-1)=a,$$

因此 f 是满射.

设 $a_1,a_2\in R$ 且 $a_1\neq a_2$，若 $f(a_1)=f(a_2)$，即若 $a_1-1=a_2-1$，则 $a_1-1+1=a_2-1+1$，于是 $a_1=a_2$，与 $a_1\neq a_2$ 矛盾，因此当 $a_1\neq a_2$ 时，必有 $f(a_1)\neq f(a_2)$. 故 f 是内射. 所以 f 是双射.

对于任意 $a,b\in R$，有

$$f(a+b)=a+b-1;$$

$$\begin{aligned}f(a)\oplus f(b)&=(a-1)\oplus(b-1)=(a-1)+(b-1)+1\\&=(a+b-1)+((-1)+1)=a+b-1.\end{aligned}$$

因此 $f(a+b)=f(a)\oplus f(b)$. 又 $f(a\cdot b)=a\cdot b-1$，故

$$\begin{aligned}f(a)\odot f(b)&=(a-1)\odot(b-1)=(a-1)\cdot(b-1)\\&\quad+(a-1)+(b-1)\\&=a\cdot b+(-1)\cdot b+a\cdot(-1)+(-1)\cdot(-1)\\&\quad+a-1+b-1\\&=a\cdot b-b-a+1+a-1+b-1\text{(参见例 6-5)}\\&=a\cdot b-1,\end{aligned}$$

因此 $f(a\cdot b)=f(a)\odot f(b)$.

由上可知，f 是由环 $\langle R;+,\cdot\rangle$ 到环 $\langle R;\oplus,\odot\rangle$ 的同构.

第七章　格和布尔代数

7.1　内容提要

1. 格的基本概念

• 偏序集、上界、下界、最大下界、最小上界、最小元素、最大元素；

• 最大下界和最小上界若存在，则唯一；

• 最小元素、最大元素若存在，则唯一；

• 格，子格.

2. 格的性质

• 格的十条基本性质；

• 格的对偶原理；

• 格中的运算$\vee$，$\wedge$满足交换律，结合律，等幂律，吸收律；

• 格的保序性.

3. 特殊的格

• 分配格；

• 有界格；

• 有补格；

• 有补分配格，布尔代数.

4. 布尔代数的性质

• 布尔代数中运算$\vee$，$\wedge$，$-$，满足十条基本性质，其中交换

律，分配律，分配律，同一律和互补律独立；

• 原子；

• 有限布尔代数$\langle B;-,\vee,\wedge\rangle$同构于一集合代数$\langle 2^M;',\cup,\cap\rangle$.

5. 布尔表达式

7.2 基本知识点

1. 偏序集

例 7-1 设$L=\{1,2,\cdots,12\}$，在L上定义整除关系.

(1)$\langle L;|\rangle$是否是偏序集，若是，画出其 Hasse 图；

(2)在L中找 8 与 12 的最大下界和最小上界，4 与 6 的最大下界和最小上界；

(3)在L中找最小元素和最大元素.

解 (1)因为在L上整除关系"|"满足自反，反对称，传递性，所以$\langle L;|\rangle$是偏序集，其 Hasse 图如图 7-1 所示.

(2)因为$1|8,2|8,4|8,1|12,2|12,4|12$，所以 1，2，4 均是 8 与 12 的下界，但由于$1|4,2|4$，故 4 是最大下界.

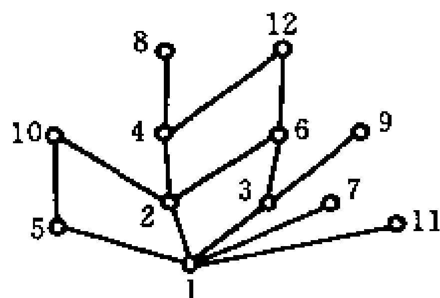


图 7-1

在L中设有元素a能满足$8|a$，且$12|a$，故 8 与 12 无上界，从而无最小上界.

另一方面，因为$1|4,2|4,1|6,2|6$，所以 1，2 均是 4 与 6 的下界，但由于$1|2$，因此 2 是 4 与 6 的最大下界.

因为$4|12,6|12$，所以 12 是 4 与 6 的上界，在L中设有元素b能满足$4|b,6|b$，且$b|12$，所以 12 是

4 与 6 的最小上界.

(3)因为对任意的 $a\in L,1|a$,所以 1 是 L 的最小元素.

在 L 中没有元素 x 能满足,对任意 $l\in L,l|x$,所以 L 无最大元素.

2. 格

$\langle L;\leqslant\rangle$是格要满足两个条件:

(1)$\langle L,\leqslant\rangle$是一个偏序集;

(2)对 L 中任意一对元素 l_1,l_2 均存在最大下界和最小上界,分别用 $l_1\wedge l_2=\mathrm{glb}(l_1,l_2),l_1\vee l_2=\mathrm{lub}(l_1,l_2)$表示.

例 7-2 由图 7-2 所示的偏序集$\langle L;\leqslant\rangle$,哪一个是格?为什么?

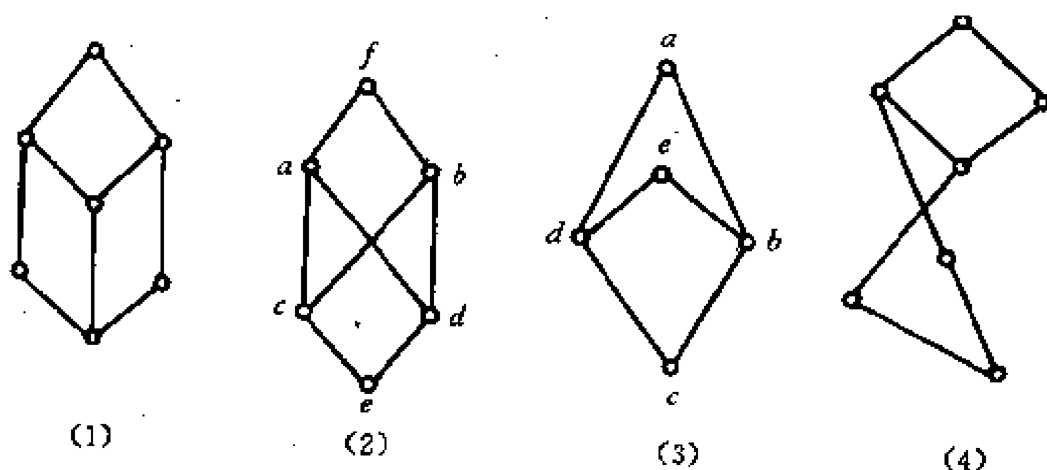


图 7-2

解 (1),(4)图所表示的偏序集是格,因为 L 中任意两元素均有最大下界和最小上界.

(2)图所表示的偏序集不是格,因为 c 与 d 有上界 a,b 和 f,但由于 a 与 b 不可比较(即 $a\leqslant b$,且 $b\leqslant a$),所以 c 与 d 无最小上界. 故不是格.

(3)图所表示的偏序集也不是格,因为 e 与 a 没有最大下界.

3. 格的十条基本性质

自反性在格$\langle L;\leqslant\rangle$中，对任意的$l_1,l_2,l_3\in L$有

$$l_1\leqslant l_1 \tag{7-1}$$

$$l_1\geqslant l_1 \tag{7-1'}$$

反对称性

若　$l_1\leqslant l_2, l_2\leqslant l_1$，则$l_1=l_2$.　(7-2)

若　$l_1\geqslant l_2, l_2\geqslant l_1$，则$l_1=l_2$.　(7-2')

传递性　若　$l_1\leqslant l_2, l_2\leqslant l_3$，则$l_1\leqslant l_3$.　(7-3)

若　$l_1\geqslant l_2, l_2\geqslant l_3$，则$l_1\geqslant l_3$.　(7-3')

下界　$l_1\wedge l_2\leqslant l_1, l_1\wedge l_2\leqslant l_2$;　(7-4)

上界　$l_1\vee l_2\geqslant l_1, l_1\vee l_2\geqslant l_2$.　(7-4')

最大下界　若　$l_3\leqslant l_1, l_3\leqslant l_2$ 则 $l_3\leqslant l_1\wedge l_2$.　(7-5)

最小上界　若　$l_3\geqslant l_1, l_3\geqslant l_2$ 则 $l_3\geqslant l_1\vee l_2$.　(7-5')

对偶式：在格中，一个含有格的元素和符号$=,\leqslant,\geqslant,\vee,\wedge$的关系式$P$中，用$\geqslant$代替$\leqslant$，用$\leqslant$代替$\geqslant$，用$\wedge$代替$\vee$，用$\vee$代替$\wedge$就得到一个新的关系式$P^D$，$P^D$称为$P$的对偶式.

(7-1)～(7-5)与(7-1')～(7-5')对应的式子互为对偶.

对偶定理　对于格$\langle L;\leqslant\rangle$上的任一真命题，其对偶亦为真.

定理 7.3.1　设$\langle L;\leqslant\rangle$是格，对任意的$l_1,l_2\in L$，有$(l_1\vee l_2=l_2)\Leftrightarrow(l_1\wedge l_2=l_1)\Leftrightarrow(l_1\leqslant l_2)$.

例 7-3　试证明在格中若$a\leqslant b\leqslant c$，则

(1)$a\vee b=b\wedge c$;

(2)$(a\wedge b)\vee(b\wedge c)=(a\vee b)\wedge(b\vee c)$.

证　(1)因为$a\leqslant b$，由定理 7.3.1 知$a\vee b=b$.

因为$b\leqslant c$，所以$b\wedge c=b$，因此

$$a\vee b=b\wedge c.$$

(2)因为$a\leqslant b$，所以$a\wedge b=a, a\vee b=b$. 又因为$b\leqslant c$，所以$b\wedge c$

$=b, b\vee c=c$. 于是

$$(a\wedge b)\vee(b\wedge c)=a\vee b=b;$$

$$(a\vee b)\wedge(b\vee c)=b\wedge c=b;$$

$$(a\wedge b)\vee(b\wedge c)=(a\vee b)\wedge(b\vee c).$$

例 7-4 设$\langle L;\leqslant\rangle$是格,对任意的$a,b,c\in L$,有$(a\wedge b)\vee(b\wedge c)\leqslant(a\vee b)\wedge(b\vee c)$.

证 因为$a\wedge b\leqslant b, b\wedge c\leqslant b$,所以

$$(a\wedge b)\vee(b\wedge c)\leqslant b \tag{1}$$

又因为$b\leqslant(a\vee b), b\leqslant(b\vee c)$,所以

$$b\leqslant(a\vee b)\wedge(b\vee c) \tag{2}$$

由(1),(2)根据传递性得

$$(a\wedge b)\vee(b\wedge c)\leqslant(a\vee b)\wedge(b\vee c).$$

4. 格的性质

设$\langle L;\leqslant\rangle$是一个格,则对任意$l_1,l_2,l_3\in L$,有

(1)交换律$l_1\vee l_2=l_2\vee l_1, l_1\wedge l_2=l_2\wedge l_1$;

(2)结合律$l_1\vee(l_2\vee l_3)=(l_1\vee l_2)\vee l_3$,
$l_1\wedge(l_2\wedge l_3)=(l_1\wedge l_2)\wedge l_3$;

(3)等幂律$l_1\vee l_1=l_1$,　　$l_1\wedge l_1=l_1$;

(4)吸收律$l_1\vee(l_1\wedge l_2)=l_1$,　　$l_1\wedge(l_1\vee l_2)=l_1$.

定理 7.4.1:在格$\langle L;\leqslant\rangle$中,对任意的$l_1,l_2,l_3,l_4\in L$,若$l_1\leqslant l_3, l_2\leqslant l_4$,则$l_1\vee l_2\leqslant l_3\vee l_4, l_1\wedge l_2\leqslant l_3\wedge l_4$.

推论:在格$\langle L;\leqslant\rangle$中,对于任意的$l_1,l_2,l_3\in L$,若$l_2\leqslant l_3$,则$l_1\vee l_2\leqslant l_1\vee l_3, l_1\wedge l_2\leqslant l_1\wedge l_3$.

例 7-5 设$\langle L;\leqslant\rangle$是一个格,试证对任意元素$a,b,c\in L$,有

$$a\vee[(a\vee b)\wedge(a\vee c)]=(a\vee b)\wedge(a\vee c)$$

分析 在格中要证明等式成立,通常证"左式"$\leqslant$"右式"和"右式"$\leqslant$"左式"然后利用反对称性得"左式"="右式"

证法一 对$\forall\ a,b,c\in L$.

由上界(7-4′)知 $a \vee b \geqslant a, a \vee c \geqslant a$.

根据定理 7.4.1 和等幂律可得

$$(a \vee b) \wedge (a \vee c) \geqslant a \wedge a = a.$$

又 $(a \vee b) \wedge (a \vee c) \geqslant (a \vee b) \wedge (a \vee c)$，所以

$$a \vee [(a \vee b) \wedge (a \vee c)] \leqslant (a \vee b) \wedge (a \vee c).$$

另一方面由上界的(7-4′)知

$$(a \vee b) \wedge (a \vee c) \leqslant a \vee [(a \vee b) \wedge (a \vee c)],$$

$$(a \vee b) \wedge (a \vee c) = a \vee [(a \vee b) \wedge (a \vee c)].$$

证法二 对 $\forall a,b,c \in L$，由上界(7-4′)知 $a \vee b \geqslant a, a \vee c \geqslant a$，所以，由定理 7.4.1 和等幂律得

$$a = a \wedge a \leqslant (a \vee b) \wedge (a \vee c).$$

再由定理 7.3.1 得

$$a \vee [(a \vee b) \wedge (a \vee c)] = (a \vee b) \wedge (a \vee c).$$

证法三 对 $\forall a,b,c \in L$，根据结合律，吸收律有

$$a \wedge [(a \vee b) \wedge (a \vee c)] = [a \wedge (a \vee b)] \wedge (a \vee c) = a \wedge (a \vee c) = a.$$

由定理 7.3.1 知 $a \leqslant (a \vee b) \wedge (a \vee c)$，所以

$$a \vee [(a \vee b) \wedge (a \vee c)] = (a \vee b) \wedge (a \vee c).$$

5. 格的另一定义形式

格除前面按偏序定义外，还有按代数系统定义的另一种形式.

给定 $\langle L; \vee, \wedge \rangle$ 是一个代数系统，若 L 上的二个二元运算 $\vee$、$\wedge$ 满足结合律、交换律和吸收律，则 $\langle L; \vee, \wedge \rangle$ 是一个格.

可以证明，给定一个格 $\langle L; \leqslant \rangle$，由 L 上定义的最小上界运算 $\vee$ 和最大下界运算 $\wedge$，能得其另一表示形式 $\langle L; \vee, \wedge \rangle$，称为由 $\langle L; \leqslant \rangle$ 诱导的代数格. 另一方面，给定一个格 $\langle L; \vee, \wedge \rangle$ 也可由二元运算 $\vee$ 和 $\wedge$ 引入一偏序"$\leqslant$"，使 $\langle L; \leqslant \rangle$ 为格，对任意 $l_1, l_2 \in L$，当且仅当 $l_1 \vee l_2 = l_1$ 时，$l_2 \leqslant l_1$，因此，两种格的定义形式等价.

若 $\langle A; \vee, \wedge \rangle$ 是 $\langle L; \vee, \wedge \rangle$ 的子代数，则称 $\langle A; \vee, \wedge \rangle$ 是 $\langle L;$

$\vee,\wedge$〉的子格.

例 7-6 设 $B=\{0,1\}$，$B^3=\{(a_1,a_2,a_3)|a_i\in B\}$，证明〈$B^3$；$\vee,\wedge$〉是一个格，其中，对任意的$(a_1,a_2,a_3)$，$(b_1,b_2,b_3)\in B^3$，有

$$(a_1,a_2,a_3)\vee(b_1,b_2,b_3)=(\max\{a_1,b_1\},\max\{a_2,b_2\},\max\{a_3,b_3\});$$

$$(a_1,a_2,a_3)\wedge(b_1,b_2,b_3)=(\min\{a_1,b_1\},\min\{a_2,b_2\},\min\{a_3,b_3\}).$$

解 由定义知$\vee,\wedge$是B上的二元运算.因为对$\forall\ a,b,c\in B$，有

$$\max\{a,b\}=\max\{b,a\},\min\{a,b\}=\min\{b,a\},$$

$$\max\{a,\max\{b,c\}\}=\max\{\max\{a,b\},c\}=\max\{a,b,c\},$$

$$\min\{a,\min\{b,c\}\}=\min\{\min\{a,b\},c\}=\min\{a,b,c\};$$

所以$\wedge,\vee$满足交换律和结合律.

又对任意的(a_1,a_2,a_3)，$(b_1,b_2,b_3)\in B^3$，有

$$\begin{aligned}&(a_1,a_2,a_3)\wedge[(a_1,a_2,a_3)\vee(b_1,b_2,b_3)]\\=&(a_1,a_2,a_3)\wedge(\max\{a_1,b_1\},\max\{a_2,b_2\},\max\{a_3,b_3\})\\=&(\min\{a_1,\max\{a_1,b_1\}\},\min\{a_2,\max\{a_2,b_2\}\},\\&\min\{a_3,\max\{a_3,b_3\}\}).\end{aligned}$$

若$a_1\geqslant b_1$，则

$$\min\{a_1,\max\{a_1,b_1\}\}=\min\{a_1,a_1\}=a,$$

若$a_1<b_1$，则

$$\min\{a,\max\{a_1,b_1\}\}=\min\{a_1,b_1\}=a,$$

所以 $(a_1,a_2,a_3)\wedge[(a_1,a_2,a_3)\vee(b_1,b_2,b_3)]=(a_1,a_2,a_3)$.

类似可证

$$(a_1,a_2,a_3)\vee[(a_1,a_2,a_3)\wedge(b_1,b_2,b_3)]=(a_1,a_2,a_3).$$

所以$\wedge,\vee$满足吸收律，故〈B^3；$\vee,\wedge$〉是一个格.

例 7-7 设〈L；$\leqslant$〉是格，其 Hasse 图如图 7-3 所示，取 $S_1=\{a,b,c,d\}S_2=\{a,b,d,f\}$，$S_3=\{b,c,d,f\}$，问〈$S_1$；$\leqslant$〉，〈$S_2$；$\leqslant$〉，〈$S_3$；$\leqslant$〉中哪些是格？哪些是〈$L$；$\leqslant$〉的子格.

解 (1)对$\forall\ x,y\in S_1$，由 Hasse 图知 $\mathrm{glb}(x,y)=x\wedge y\in S_1$，$\mathrm{lub}(x,y)=x\vee y\in S_1$.

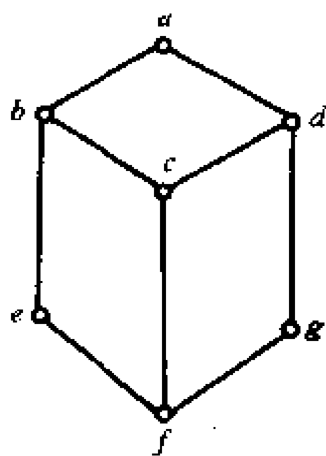


图 7-3

$\therefore \langle S_1; \leqslant \rangle$是格，且是$\langle L; \leqslant \rangle$的子格.

(2)$b, d \in S_2$，$\mathrm{glb}(b,d)=f \in S_2$，$\mathrm{lub}(b,d)=a \in S_2$ 可以验证 S_2 中，任意两元素的最大下界和最小上界存在，所以$\langle S_2; \leqslant \rangle$是格. 但在 S_2 中，$\mathrm{glb}(b,d)=f$ 不等于 L 中 $\mathrm{glb}(b,d)=c$，即$\wedge$在 S_2 中不封闭. 因此，$\langle S_2; \leqslant \rangle$不是$\langle L; \leqslant \rangle$的子格.

(3)b, d 在 S_3 中无最小上界，故$\langle S_3; \leqslant \rangle$不是格.

6. 分配格与有补格

若一个格$\langle L; \vee, \wedge \rangle$满足分配律，则称为分配格. 即对任意 $l_1, l_2, l_3 \in L$，下述两等式之一成立.

$$l_1 \wedge (l_2 \vee l_3) = (l_1 \wedge l_2) \vee (l_1 \wedge l_3);$$

$$l_1 \vee (l_2 \wedge l_3) = (l_1 \vee l_2) \wedge (l_1 \vee l_3).$$

注：这两个等式是等价的，若一个成立，另一个也成立.

有界格 如果一个格有最大元素和最小元素，则称它为有界格. 其最大元素和最小元素分别用“1”和“0”表示.

补元 设$\langle L; \vee, \wedge \rangle$是有界格，若对任意的 $l \in L$，存在 $\bar{l} \in L$，使得 $l \vee \bar{l} = 1$ $l \wedge \bar{l} = 0$，则称元素 $\bar{l}$ 是 l 的补.

有补格 设$\langle L; \vee, \wedge \rangle$是有界格，如果 L 中每一个元素都有补，则称$\langle L; \vee, \wedge \rangle$为有补格.

有补分配格 如果一个格既是有补格又是分配格，则称为有补分配格.

定理 7.6.1 在有补分配格$\langle L; \vee, \wedge \rangle$中，任一元素 $l \in L$ 的补元素是唯一的.

例 7-8 如图 7-4 所示的几个次序图均是格，哪个是分配

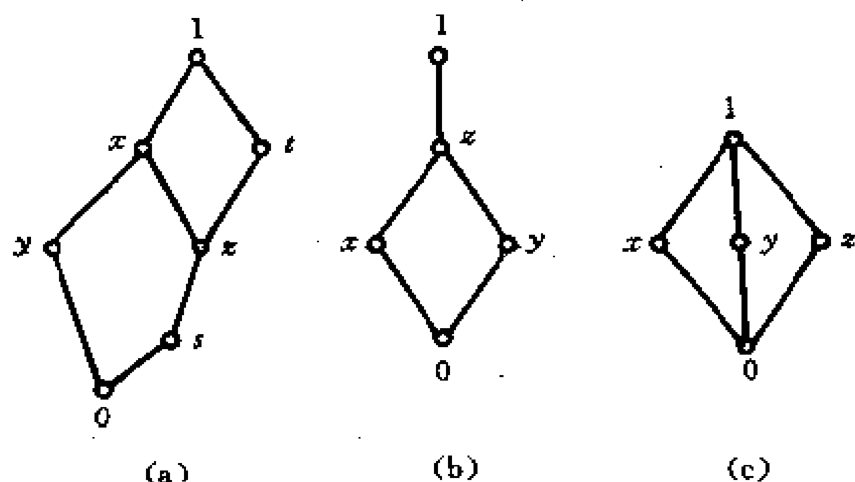


图 7-4

格？哪个是有补格？

解 这三个格均是有界格.

(1)因为(a)中 x 无补元，故它不是有补格.

又因为

$$z \wedge (y \vee s) = z \wedge x = z;$$

$$(z \wedge y) \vee (z \wedge s) = 0 \vee s = s.$$

所以 $z \wedge (y \vee s) \neq (z \wedge y) \vee (z \wedge s)$，故(a)也不是分配格.

(2)因为(b)中 z 无补元，故它不是有补格. 可以验证，(b)中任意三元素满足分配等式，故是分配格.

(3)(c)中 0,1 互补，x,y,z 两两互补，故(c)是一有补格. 又因为

$$x \wedge (y \vee z) = x \wedge 1 = x,$$

$$(x \wedge y) \vee (x \wedge z) = 0 \vee 0 = 0,$$

所以

$$x \wedge (y \vee z) \neq (x \wedge y) \vee (x \wedge z),$$

故(c)不是分配格.

7. 布尔代数

布尔代数 一个有补分配格.

布尔代数$\langle B;-,\vee,\wedge\rangle$，其中$\vee,\wedge$是格中并、交运算，"$-$"是求补运算，布尔代数满足十条基本运算定律：交换律，结合律，等幂律，吸收律，分配律，同一律，零一律，互补律，对合律，德·摩根定律.

布尔代数的第二种定义形式：设$\langle B;-,\vee,\wedge\rangle$为一个代数系，"$-$"为定义在$B$上的一元运算，$\vee,\wedge$为定义在$B$上的二元运算，若它们满足交换律，分配律，同一律和互补律，则称B为布尔代数.

定理 7.7.1 布尔代数的每一子代数仍是布尔代数.

例 7-9 考察代数系统$\langle F;-,\vee,\wedge\rangle$，这里$F=\{f\mid f:N\to\{0,1\}\}$，对于任意的$f_1,f_2\in F$，有

当且仅当$f_1(n)=0$时，$\bar{f}_1(n)=1$；

当且仅当$f_1(n)=1$或$f_2(n)=1$时，$(f_1\vee f_2)(n)=1$；

当且仅当$f_1(n)=1$且$f_2(n)=1$时，$(f_1\wedge f_2)(n)=1$；

试证明$\langle F;-,\vee,\wedge\rangle$是布尔代数.

解 对任意的$f_1,f_2,f_3\in F$. 对任意的$n\in N$

(1)因为

$$(f_1\vee f_2)(n)=\begin{cases}0, & \text{当 } f_1(n)=0 \text{ 且 } f_2(n)=0 \text{ 时；}\\ 1, & \text{其他；}\end{cases}$$

$$(f_2\vee f_1)(n)=\begin{cases}0, & \text{当 } f_1(n)=0 \text{ 且 } f_2(n)=0 \text{ 时；}\\ 1, & \text{其他，}\end{cases}$$

所以，
$$f_1\vee f_2=f_2\vee f_1.$$

类似可证 $f_1\wedge f_2=f_2\wedge f_1$，因此，交换律满足.

(2)因为

$$(f_1\wedge(f_2\vee f_3))(n)$$
$$=\begin{cases}1, & \text{当 } f_1(n)=1 \text{ 且}(f_2(n)=1 \text{ 或 } f_3(n)=1)\text{ 时；}\\ 0, & \text{当 } f_1(n)=0 \text{ 或}(f_2(n)=0 \text{ 且 } f_3(n)=0)\text{ 时，}\end{cases}$$

$$(f_1\wedge f_2)(n)=\begin{cases}1, & \text{当 } f_1(n)=f_2(n)=1 \text{ 时；}\\ 0, & \text{其他.}\end{cases}$$

$$(f_1 \wedge f_3)(n) = \begin{cases} 1, 当\ f_1(n) = f_3(n) = 1\ 时; \\ 0, 其他, \end{cases}$$

而

$$((f_1 \wedge f_2) \vee (f_1 \wedge f_3))(n)$$

$$= \begin{cases} 1, & 当\ f_1(n) = 1\ 且(f_2(n) = 1\ 或\ f_3(n) = 1); \\ 0, & 当\ f_1(n) = 0\ 或(f_2(n) = 0\ 且\ f_3(n) = 0), \end{cases}$$

所以

$$f_1 \wedge (f_2 \vee f_3) = (f_1 \wedge f_2) \vee (f_1 \wedge f_3).$$

类似可证 $f_1 \vee (f_2 \wedge f_3) = (f_1 \vee f_2) \wedge (f_1 \vee f_3)$. 因此,分配律成立.

(3)令 $O_f: N \longrightarrow \{0,1\}$,对任意 $n \in N$,有 $O_f(n) = 0$.

$I_f: N \longrightarrow \{0,1\}$,对任意 $n \in N$,有 $I_f(n) = 1$.

显然 $O_f, I_f \in F$,且对任意 $f \in F$. 因为

$$(f \vee O_f)(n) = f(n) \vee O_f(n) = f(n) \vee 0 = f(n);$$

$$(f \wedge I_f)(n) = f(n) \wedge I_f(n) = f(n) \wedge 1 = f(n),$$

所以,$f \vee O_f = f, f \wedge I_f = f$,同一律成立.

(4)对任意的 $f \in F$,因为 $f(n) = 0$,当且仅当 $\bar{f}(n) = 1$,所以

$$(f \wedge \bar{f})(n) = f(n) \wedge \bar{f}(n) = 0 = O_f(n);$$

$$(f \vee \bar{f})(n) = f(n) \vee \bar{f}(n) = 1 = I_f(n),$$

故 $f \wedge \bar{f} = O_f, f \vee \bar{f} = I_f$,互补律成立,因此$\langle F; -, \vee, \wedge \rangle$是一个布尔代数.

例 7-10 设$\langle B; ', \vee, \wedge \rangle$为布尔代数,$\# B \geq 2$,任取 $a \in B, a \neq 0, a \neq 1$,证明$\langle T; ', \vee, \wedge \rangle$是 B 的一子代数,且是布尔代数,其中 $T = \{0, a, a', 1\}$.

解 对 T 中各元素的运算表如表 7-1 所示.

由 B 是布尔代数知

由下述运算表知,T 对 $\vee, \wedge, '$封闭,故是 B 的子代数. 故根据定理 7.7.1 知$\langle T; \vee, \wedge, ' \rangle$也是一布尔代数.

表 7-1

$\vee$	0	a	a'	1
0	0	a	a'	1
a	a	a	1	a
a'	a'	1	a'	a
1	1	1	1	1

$\wedge$	0	a	a'	1
0	0	0	0	0
a	0	a	0	a
a'	0	0	a'	a'
1	0	a	a'	1

1	
0	1
a	a'
a'	a
1	0

8. 原子及有限布尔代数

原子　在布尔代数$\langle B;-,\vee,\wedge\rangle$中，如果元素$a\neq0$，且对每一个$x\in B$，有$x\wedge a=a$或$x\wedge a=0$，则称$a$是原子.

即若$a\neq0$,$a\in B$是原子，那么a与B中任意元素x，要么$a\leqslant x$，要么$x=0$或a与x不可比较.即原子是仅比0元素“大”一点的元素(这里“大”是按偏序关系比较).

定理 7.8.1　设$\langle B;-,\vee,\wedge\rangle$是一有限布尔代数，则对任意$x\in B$，且$x\neq0$，一定存在一个原子$a$，使得$a\leqslant x$.

定理 7.8.2　在布尔代数$\langle B;-,\vee,\wedge\rangle$中，任意两原子$a_1$和$a_2$，若$a_1\wedge a_2\neq0$，则$a_1=a_2$.

定理 7.8.3　设$\langle B;-,\vee,\wedge\rangle$是一有限布尔代数，任意的$x\in B$且$x\neq0$，$a_1,a_2,\cdots,a_n$是$\langle B;-,\vee,\wedge\rangle$中满足$a_i\leqslant x$的所有原子，则$x=a_1\vee a_2\vee\cdots\vee a_n$，且表示方式唯一.

定理 7.8.4　设$\langle B;-,\vee,\wedge\rangle$是一有限布尔代数，$M$是该代数所有原子的集合，则$\langle B;-,\vee,\wedge\rangle$与$\langle z^M;,\cup,\cap\rangle$同构.

定理 7.8.5　每一有限布尔代数的元素个数必为2的幂.

例 7-11　设$S=\{1,2,3,5,6,10,15,30\}$，在S上定义整除关系“1”，则$\langle S;|\rangle$是一个有补分配格，即布尔代数，求其所有的原子，以及$x=10$，$x=15$的原子表达式.

解　$\langle S;1\rangle$的 Hasse 图如图 7-5 所示.

由 Hasse 图可验证$\langle S;|\rangle$是一有补分配格，即布尔代数，最小

元素是 1，最大元素是 30.

因为 $a=2\neq 1$（最小元素，相当于 0），且对任意 $x\in B$、$x\wedge 2=2$ 或 $x\wedge 2=1$，所以，2 是原子. 类似可验证 3，5 也是原子，该布尔代数 $\langle S;', \vee, \wedge\rangle=\langle S;|\rangle$ 的所有原子为 2，3，5.

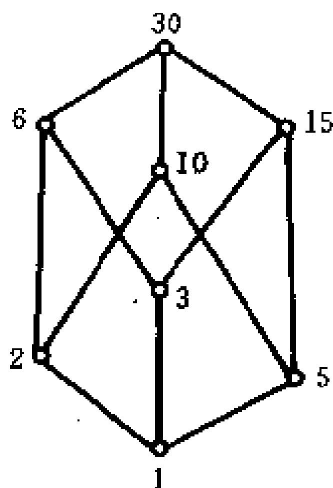


图 7-5

$x=10$ 和 $x=15$ 的原子表示式分别为 $10=2\vee 5$，$15=3\vee 5$.

例 7-12 设 $a, b_1, b_2, \cdots, b_r$ 都是有限布尔代数 $\langle B;-, \vee, \wedge\rangle$ 的原子，证明当且仅当存在 $i(1\leqslant i\leqslant r)$ 使得 $a=b_i$ 时，有 $a\leqslant b_1\vee b_2\vee\cdots\vee b_r$.

证 **必要性** 设存在 $i(1\leqslant i\leqslant r)$ 使 $a=b_i$，则 $b_i\leqslant b_1\vee b_2\vee\cdots\vee b_r$，所以 $a=b_i\leqslant b_1\vee b_2\vee\cdots\vee b_r$

充分性 设 $a\leqslant b_1\vee b_2\vee\cdots\vee b_r$，

用反证法，若不存在 $i(1\leqslant i\leqslant r)$ 使 $a=b_i$，则由于 $a, b_1, b_2, \cdots, b_r$ 均是原子，故根据定理 7.8.2 知 $a\wedge b_1=0, a\wedge b_2=0, \cdots, a\wedge b_r=0$，所以

$$a\wedge(b_1\vee b_2\vee\cdots\vee b_r)=(a\wedge b_1)\vee(a\wedge b_2)\vee\cdots\vee(a\wedge b_r)=0$$

又 $a\leqslant b_1\vee b_2\vee\cdots\vee b_r$，则由定理 7.3.1 知

$a\wedge(b_1\vee b_2\vee\cdots\vee b_r)=a$，而 a 是原子，所以 $a\neq 0$，即 $a\wedge(b_1\vee b_2\vee\cdots\vee b_r)\neq 0$ 与上述结论矛盾. 所以必是假设错误，故存在 $i(1\leqslant i\leqslant r)$ 使 $a=b_i$.

例 7-13 作出满足下述要求的六元素格，(1)全序；(2)有补格；(3)分配格. 是否有六元素的布尔代数？

解 满足要求的各六元素格的 Hasse 图如图 7-6 所示.

由于 6 不是 2 的幂，所以没有六个元素的布尔代数.

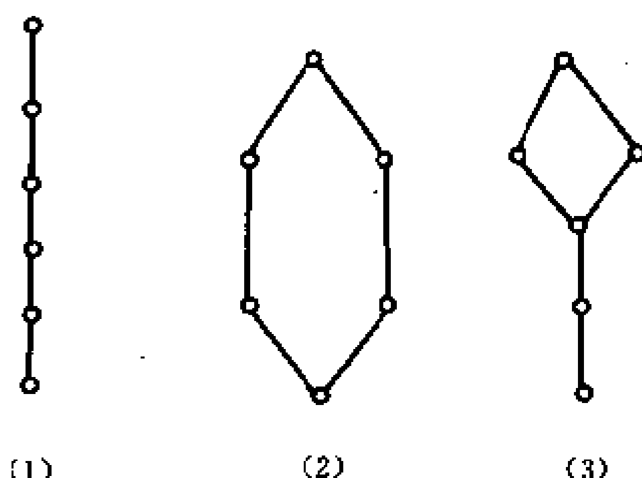


图 7-6

9. 布尔表达式

例 7-14 设 $f(x,y)=(x\wedge(\alpha\vee y))\vee(\bar{x}\wedge\bar{y})$是布尔代数 $\langle\{0,\alpha,\beta,1\};-,\vee,\wedge\rangle$上,由 x,y 产生的一个布尔表达式,求 $f(x,y)$的最小项标准形式.

解
$$f(0,0)=(0\wedge(\alpha\vee 0))\vee(\bar{0}\wedge\bar{0})=1;$$
$$f(0,1)=(0\wedge(\alpha\vee 1))\vee(\bar{0}\wedge\bar{1})=0\vee(1\wedge 0)=0;$$
$$f(1,0)=(1\wedge(\alpha\vee 0))\vee(\bar{1}\wedge\bar{0})=(1\wedge\alpha)\vee(0\wedge 1)=\alpha;$$
$$f(1,1)=(1\wedge(\alpha\vee 1))\vee(\bar{1}\wedge\bar{1})=(1\wedge 1)\vee 0=1.$$

$f(x,y)$的最小标准形式
$$f(x,y)=(f(0,0)\wedge\bar{x}\wedge\bar{y})\vee(f(0,1)\wedge\bar{x}\wedge y)\vee(f(1,0)\wedge x\wedge\bar{y})\vee(f(1,1)\wedge x\wedge y)$$
$$=(1\wedge\bar{x}\wedge\bar{y})\vee(\alpha\wedge x\wedge\bar{y})\vee(1\wedge x\wedge y).$$

7.3 问答与论证

例 7-15 设$\langle L;\leqslant\rangle$是一个格，$a,b\in L$，且$a<b$（即$a\leqslant b$，但$a\neq b$），令集合$B=\{x\mid x\in L$，且$a\leqslant x\leqslant b\}$试证明$\langle B;\leqslant\rangle$是$\langle L;\leqslant\rangle$的一个子格.

证 因为$\langle L;\leqslant\rangle$是格，所以$L$上由偏序"$\leqslant$"可导出二个二元运算$\vee$，$\wedge$，即对任意的$l_1,l_2\in L$，有$l_1\wedge l_2=\text{glb}(l_1,l_2)$，$l_1\vee l_2=\text{lub}(l_1,l_2)$.

由B的定义知$B\subseteq L$，$a\in B$，所以$B\neq\varnothing$.

对任意的$x,y\in B$，由于$\langle L;\leqslant\rangle$是格，所以$x\wedge y$和$x\vee y$在$L$中存在且唯一.

下面证$x\wedge y\in B$，$x\vee y\in B$.

由B的定义知 $a\leqslant x\leqslant b$，$a\leqslant y\leqslant b$.

所以$a\leqslant x$且$a\leqslant y$，根据定理 7.4.1 及等幂律得$a=a\wedge a\leqslant x\wedge y$，所以$a\leqslant x\wedge y$.

类似地由$x\leqslant b$，$y\leqslant b$得$x\wedge y\leqslant b$，所以$a\leqslant x\wedge y\leqslant b$，即$x\wedge y\in B$.

类似地可证得 $a\leqslant x\vee y\leqslant b$. 即$x\vee y\in B$

因此，$\vee$，$\wedge$在B上封闭，故$\langle B;\vee,\wedge\rangle$是$\langle L;\vee,\wedge\rangle=\langle L;\leqslant\rangle$的子代数，从而$\langle B;\leqslant\rangle=\langle B;\vee,\wedge\rangle$是$\langle L;\leqslant\rangle$的一个子格.

例 7-16 试证明在具有两个或更多个元素的格中，不会有元素是它自身的补.

证 设$\langle L;\leqslant\rangle$是一个格，$\# L\geqslant 2$.

用反证法 假定存在$l\in L$ 使得$l\wedge l=0$，$l\vee l=1$，则由幂等律知$l=0=1$与$\# L\geqslant 2$矛盾. 所以，L中必不存在元素是它自身的补.

例 7-17 设$\langle L;\leqslant\rangle$是一有界分配格，$L_1$是$L$中所有具有补元的元素组成的集合. 试证明$\langle L_1;\leqslant\rangle$是$\langle L;\leqslant\rangle$的子格.

证 对任意 $l_1, l_2 \in L_1$，即∃ $\bar{l}_1, \bar{l}_2 \in L$ 使 $l_1 \wedge \bar{l}_1 = 0, l_1 \vee \bar{l}_1 = 1, l_2 \wedge \bar{l}_2 = 0, l_2 \vee \bar{l}_2 = 1$.

$$(l_1 \vee l_2) \wedge (\bar{l}_1 \wedge \bar{l}_2) = (l_1 \wedge \bar{l}_1 \wedge \bar{l}_2) \vee (l_2 \wedge \bar{l}_1 \wedge \bar{l}_2)$$
$$= 0 \vee 0 = 0$$
$$(l_1 \vee l_2) \vee (\bar{l}_1 \wedge \bar{l}_2) = (l_1 \vee l_2 \vee \bar{l}_1) \wedge (l_1 \vee l_2 \vee \bar{l}_2)$$
$$= 1 \vee 1 = 1$$

所以 $\overline{l_1 \vee l_2} = \bar{l}_1 \wedge \bar{l}_2, l_1 \vee l_2 \in L_1$.

类似地

$$(l_1 \wedge l_2) \wedge (\bar{l}_1 \vee \bar{l}_2) = (l_1 \wedge l_2 \wedge \bar{l}_1) \vee (l_1 \wedge l_2 \wedge \bar{l}_2) = 0;$$
$$(l_1 \wedge l_2) \vee (\bar{l}_1 \vee \bar{l}_2) = (l_1 \vee \bar{l}_1 \vee \bar{l}_2) \wedge (l_2 \vee \bar{l}_1 \vee \bar{l}_2)$$
$$= 1 \wedge 1 = 1.$$

所以 $\overline{l_1 \wedge l_2} = \bar{l}_1 \vee \bar{l}_2, l_1 \wedge l_2 \in L_1$.

因此 $\langle L_1; \leqslant \rangle$ 是 $\langle L; \leqslant \rangle$ 的子代数，故 $\langle L_1; \leqslant \rangle$ 是 $\langle L; \leqslant \rangle$ 的子格.

例 7-18 设 $\langle L; \leqslant \rangle$ 是一个格，如果任意 $a, b, c \in L$，则

$$[(a \wedge b) \vee (a \wedge c)] \wedge [(a \wedge b) \vee (b \wedge c)] = a \wedge b$$

证 由上界(7-4′)知

$$a \wedge b \leqslant (a \wedge b) \vee (a \wedge c);$$
$$a \wedge b \leqslant (a \wedge b) \vee (b \wedge c).$$

所以根据定理 7.4.1，有

$$(a \wedge b) \wedge (a \wedge b) \leqslant [(a \wedge b) \vee (a \wedge c)] \wedge [(a \wedge b) \vee (b \wedge c)].$$

由幂等律得

$$a \wedge b \leqslant [(a \wedge b) \vee (a \wedge c)] \wedge [(a \wedge b) \vee (b \wedge c)] \quad (1)$$

另一方面，由下界(7-4)知

$$a \wedge c \leqslant a \qquad a \wedge b \leqslant a.$$

于是由定理 7.4.1 及幂等律得

$$(a \wedge b) \vee (a \wedge c) \leqslant a \vee a = a;$$
$$(a \wedge b) \vee (b \wedge c) \leqslant b \vee b = b.$$

再根据定理 7.4.1 得

$[(a \wedge b) \vee (a \wedge c)] \wedge [(a \wedge b) \vee (b \wedge c)] \leqslant a \wedge b$. (2)

由(1)(2)即得

$[(a \wedge b) \vee (a \wedge c)] \wedge [(a \wedge b) \vee (b \wedge c)] = a \wedge b$.

例 7-19 已知 G 为群，$S(G)$为其子群的全体构成的集合，偏序关系是集合的包含关系$\subseteq$，证明$\langle S(G);\subseteq\rangle$是格. $\langle S(G);\subseteq\rangle$是否为$\langle 2^G;\subseteq\rangle$的子格？

证 (1)对任意的 $H_1, H_2 \in S(G)$，易知 $H_1 \cap H_2$ 仍是 G 的子群，所以

$$H_1 \cap H_2 = \mathrm{glb}(H_1, H_2) \in S(G).$$

但 $H_1 \cup H_2$ 不一定仍是子群，故 $\mathrm{lub}(H_1, H_2) = H$，其中 $H_1 \cup H_2 \subseteq H$，H 是包含 $H_1 \cup H_2$ 的 G 中最小子群，最坏情况 $H = G$，故 $H \in S(G)$，因此，$\langle S(G);\subseteq\rangle$是格.

(2)$\langle S(G);\subseteq\rangle$不是$\langle 2^G;\subseteq\rangle$的子格，

由于不能保证 $H_1 \cup H_2$ 仍是子群，所以，可能 H_1 与 H_2 在 $S(G)$中的最小上界 $\mathrm{lub}(H_1, H_2) = H$ 不等于 H_1 与 H_2 在 2^G 中的最小上界 $H_1 \cup H_2$. 因此，$\langle S(G);\subseteq\rangle$不是$\langle 2^G;\subseteq\rangle$的子格.

例 7-20 设有集合 A, B 和函数 $f: 2^A \to B$，$S \subseteq 2^B$ 定义为 $S = \{y \mid y = f(x), x \in 2^A\}$，试证明 S 对于集合的运算$\cup$和$\cap$构成格$\langle 2^B; \cup, \cap\rangle$的子格.

证 对任意的 $S_1, S_2 \in S$，由 S 的定义知，存在 $A_1, A_2 \in 2^A$，使 $f(A_1) = S_1$，$f(A_2) = S_2$，于是 $S_1 \cup S_2 = f(A_1) \cup f(A_2)$，容易证明 $f(A_1) \cup f(A_2) = f(A_1 \cup A_2)$，而 $A_1, A_2 \in 2^A$，所以 $A_1 \cup A_2 \in 2^A$.

由 S 的定义知 $f(A_1 \cup A_2) \in S$，所以

$$S_1 \cup S_2 = f(A_1) \cup f(A_2) = f(A_1 \cup A_2) \in S,$$

即 S 关于$\cup$运算封闭.

又$\because S_1 \subseteq B, S_2 \subseteq B$，所以 $S_1 \cap S_2 \subseteq B$. 对任意 $b \in S_1 \cap S_2$，有 $b \in S_1 = f(A_1)$

即存在 $a \in A$，使 $f(a) = b$，也就是说，对任意 $b \in S_1 \cap S_2$，存在 $a \in A$，使 $f(a) = b$.

于是令集合 $A_3=\{a\mid a\in A,f(a)=b,b\in S_1\cap S_2\}$，显然 $A_3\in 2^A$，且 $S_1\cap S_2=f(A_3)$，从而 $S_1\cap S_2\in S$.

由上可知，S 关于 $\cup$、$\cap$ 封闭，故 $\langle S;\cup,\cap\rangle$ 是 $\langle 2^B;\cup,\cap\rangle$ 的子代数，因此 $\langle S;\cup,\cap\rangle$ 是 $\langle 2^B;\cup,\cap\rangle$ 的子格.

例 7-21 在布尔代数 $\langle B;-,\vee,\wedge\rangle$ 中，对任意的 $a,b,c\in B$，有 $(a\vee b)\wedge(c\vee\bar{b})=(a\wedge\bar{b})\vee(c\wedge b)$.

证 因为 $\langle B;-,\vee,\wedge\rangle$ 是布尔代数，故十条基本定律在其上均成立，所以

$$
\begin{aligned}
(a\vee b)\wedge(c\vee\bar{b}) &= ((a\vee b)\wedge c)\vee((a\vee b)\wedge\bar{b})\text{（分配律）}\\
&=(a\wedge c)\vee(b\wedge c)\vee(a\wedge\bar{b})\vee(b\wedge\bar{b})\\
&=(a\wedge c)\vee[(b\wedge c)\vee(a\wedge\bar{b})]\\
&=(a\wedge c\wedge(b\vee\bar{b}))\vee[(b\wedge c)\vee(a\wedge\bar{b})]\\
&=(a\wedge c\wedge b)\vee(a\wedge c\wedge\bar{b})\vee(b\wedge c)\vee(a\wedge\bar{b})\\
&=[(a\wedge(c\wedge b))\vee(b\wedge c)]\vee[(a\wedge\bar{b})\wedge c]\vee(a\wedge\bar{b})\\
&=(b\wedge c)\vee(a\wedge\bar{b})=(a\wedge\bar{b})\vee(c\wedge b),
\end{aligned}
$$

即
$$(a\vee b)\wedge(c\vee\bar{b})=(a\wedge\bar{b})\vee(c\wedge b).$$

例 7-22 试证明当且仅当对于任意元素 $a,b,c\in L$，有

$(a\wedge b)\vee(b\wedge c)\vee(c\wedge a)=(a\vee b)\wedge(b\vee c)\wedge(c\vee a)$

时，格 $\langle L;\leqslant\rangle$ 是可分配格.

证 **必要性** 设 $\langle L;\leqslant\rangle$ 是分配格，则对 $\forall\, a,b,c\in L$，有

$$
\begin{aligned}
&(a\wedge b)\vee(b\wedge c)\vee(c\wedge a)\\
&=[(a\wedge b)\vee(b\wedge c)\vee c]\wedge[(a\wedge b)\vee(b\wedge c)\vee a]\\
&=[(a\wedge b)\vee c]\wedge[(b\wedge c)\vee a]\\
&=(a\vee c)\wedge(b\vee c)\wedge(b\vee a)\wedge(c\vee a)\\
&=(a\vee b)\wedge(b\vee c)\wedge(c\vee a).
\end{aligned}
$$

充分性 对任意 $a,b,c\in L$ 令 $a'=(a\vee b)\wedge(a\vee c)$，$b'=b\vee c$，$c'=a$，则 $a',b',c'\in L$，满足等式

$$
\begin{aligned}
&(a'\wedge b')\vee(b'\wedge c')\vee(c'\wedge a')\\
&=(a'\vee b')\wedge(b'\vee c')\wedge(c'\vee a') \qquad (*)
\end{aligned}
$$

于是(＊)的

$$\begin{aligned}\text{左式}&=[(a\vee b)\wedge(a\vee c)]\wedge(b\vee c)]\vee[(b\vee c)\wedge a]\\&\quad\vee[\bar{a}\wedge((a\vee b)\wedge(a\vee c))]\\&=[((a\vee b)\wedge(a\vee c))\wedge(b\vee c)]\\&\quad\vee[(b\vee c)\wedge a]\vee a &&\text{吸收律}\\&=[(a\vee b)\wedge(b\vee c)\wedge(c\vee a)]\vee a &&\text{吸收律,交换律}\\&=[(a\wedge b)\vee(b\wedge c)\vee(c\wedge a)]\vee a &&\text{已知条件}\\&=(b\wedge c)\vee a. &&\text{交换律,吸收律}\end{aligned}$$

因为 $a\leqslant a\vee b,a\leqslant a\vee c$,故 $a\leqslant(a\vee b)\wedge(a\vee c)$.

所以,$a\vee[(a\vee b)\wedge(a\vee c)]=(a\vee b)\wedge(a\vee c)$ (定理 7.3.1)

将 a',b',c' 代入(＊)的右式得

$$\begin{aligned}\text{右式}&=[((a\vee b)\wedge(a\vee c))\vee(b\vee c)]\wedge[(b\vee c)\vee a]\\&\quad\wedge[a\vee((a\vee b)\wedge(a\vee c))]\\&=(\,[((a\vee b)\wedge(a\vee c))\vee(b\vee c)]\\&\quad\wedge[(a\vee b)\wedge(a\vee c)]\,)\wedge[(b\vee c)\vee a]\\&&&\text{交换律,分配律,结合律}\\&=[(a\vee b)\wedge(a\vee c)]\wedge[(a\vee c)\vee b]\\&&&\text{吸收律,交换律,结合律}\\&=(a\vee b)\wedge[(a\vee c)\wedge((a\vee c)\vee b)]\\&=(a\vee b)\wedge(a\vee c). &&\text{吸收律}\end{aligned}$$

所以 $$a\vee(b\wedge c)=(a\vee b)\wedge(a\vee c),$$

因此,$(L;\leqslant)$是分配格.

例 7-23 设 f 是布尔代数$\langle B;-,\vee,\wedge\rangle$到布尔代数$\langle S;',\oplus,\otimes\rangle$的同态映射,两个布尔代数的最小、最大元素分别为 0,1 和 α,β.

令 $T=\{x\mid x\in B,\text{且} f(x)=\alpha\}$,

试证明

1)$0\in T$;

2)若 $a\in T$,则对$\forall\ x\in B$,只要 $x\leqslant a$,就有 $x\in T$;

3)对$\forall\ a,b\in T$,有$a\wedge b\in T$;

证　(1)对$\forall\ a\in B$,有$0=a\wedge\bar{a}\in B$. 由f是同态映射知$f(0)=f(a\wedge\bar{a})=f(a)\otimes f(\bar{a})=f(a)\otimes f'(a)=\alpha$,所以$0\in T$.

(2)若$a\in T$,则$f(a)=\alpha$.

对$\forall\ x\in B$,当$x\leqslant a$时,$x=x\wedge a$.　　　　　　(定理7.3.1)

于是$f(x)=f(x\wedge a)=f(x)\otimes f(a)=f(x)\otimes\alpha=\alpha$,所以$x\in T$.

(3)对$\forall\ a,b\in T$,有$f(a)=\alpha,f(b)=\alpha$,于是$f(a\wedge b)=f(a)\otimes f(b)=\alpha\otimes\alpha=\alpha$,所以$a\wedge b\in T$.

B. 解题思路与方法

例B-1　设有代数系统$V=\langle Z_3;\oplus_3,\odot_3\rangle$和$Z_3$上的等价关系$\rho$,

(1)证明若ρ对于$\oplus_3$满足代换性质,则ρ对于$\odot_3$一定也满足代换性质;

(2)找出Z_3上的一个等价关系,它对于$\odot_3$满足代换性质,但对于$\oplus_3$不满足.

解　$Z_3=\{0,1,2\}$,$\oplus_3$和$\odot_3$的定义分别为

$$z_1\oplus_3 z_2=\mathrm{res}_3(z_1+z_2),z_1\odot_3 z_2=\mathrm{res}_3(z_1\cdot z_2).$$

(1)**证**　对于任意的$x_1,x_2\in Z_3$,若$x_1\rho x_2$,则由ρ对$\oplus_3$满足代换性质有$(x_1\oplus_3 x_1)\rho(x_2\oplus_3 x_2)$,即

$$\mathrm{res}_3(2x_1)\rho\quad\mathrm{res}_3(2x_2),(2\odot_3 x_1)\rho(2\odot_3 x_2).$$

又由$x_1\rho x_2$,得$\mathrm{res}_3(1\cdot x_1)\rho\quad\mathrm{res}_3(1\cdot x_2)$,即$(1\odot_3 x_1)\rho(1\odot_3 x_2)$;

又由$0\rho 0$,得$\mathrm{res}_3(0\cdot x_1)\rho\quad\mathrm{res}_3(0\cdot x_2)$,即$(0\odot_3 x_1)\rho(0\odot_3 x_2)$.

于是,由$x_1\rho x_2$可得到

$$(\alpha\odot_3 x_1)\rho(2\odot_3 x_2),(1\odot_3 x_1)\rho(1\odot_3 x_2),(0\odot_3 x_1)\rho(0\odot_3 x_2).$$

由$\odot_3$的可交换性,又得到

$(x_1\odot_3 2)\rho(x_2\odot_3 2)$，$(x_1\odot_3 1)\rho(x_2\odot_3 1)$，$(x_1\odot_3 0)\rho(x_2\odot_3 0)$.
这说明对于任意的 $x_1,x_2,y\in Z_3$，若 $x_1\rho x_2$，则有

$$(y\odot_3 x_1)\rho(y\odot_3 x_2),(x_1\odot_3 y)\rho(x_2\odot_3 y).$$

因此，对于任意的 $x_1,x_2,y_1,y_2\in Z_3$，若 $x_1\rho x_2,y_1\rho y_2$，则有

$$(x_1\odot_3 y_1)\rho(x_2\odot_3 y_1),(x_2\odot_3 y_1)\rho(x_2\odot_3 y_2).$$

又由 ρ 的传递性，可得$(x_1\odot_3 y_1)\rho(x_2\odot_3 y_2)$，
故 ρ 对于$\odot_3$ 也满足代换性质.

(2)**分析**　由第二章知，任意集合 A 上的等价关系与 A 的分划呈一一对应关系. 因此考虑此题时，可利用 Z_3 上的分划来考虑，这样会直观和简单一些.

因为 Z_3 只有三个元素，所以 Z_3 上只有五个不同的分划，它们分别如图 B-1 所示. 这说明 Z_3 上只有五个不同的等价关系，按照它们与图 B-1 中的分划(a)，(b)，…，(e)的对应关系，分别记作 ρ_a，ρ_b，ρ_c，ρ_d，ρ_e.

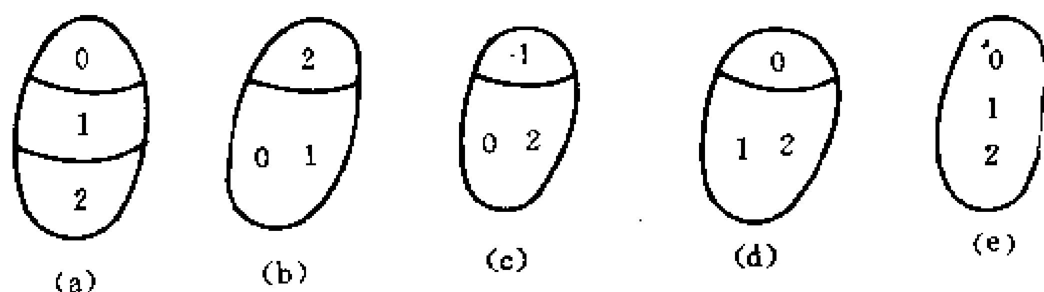


图 B-1

显然，恒等关系 ρ_a 与普遍关系 ρ_e 对于$\oplus_3$ 和$\odot_3$ 均满足代换性质.

考察分划(b)，由分划块就是等价类可知，$\alpha\rho_b\alpha$，$1\rho_b 0$，但 $\alpha\rho_b' 0$，因此$(\alpha\odot_3 1)\rho_b'(2\odot_3 0)$　($a\rho' b$ 表示$(a,b)\notin\rho$)，且$(\alpha\oplus_3 0)\rho_b'(\alpha\oplus_3 1)$. 故 ρ_b 对$\oplus_3$ 和$\odot_3$ 均不满足代换性质.

考察分划(c)，$\alpha\rho_c 2$，$0\rho_c 2$，但 $2\rho_c' 1$，$0\rho_c' 1$，因此$(2\oplus_3 0)\rho_c'(2\oplus_3 2)$，且$(2\odot_3 0)\rho_c'(2\odot_3 2)$. 故 ρ_c 对$\oplus_3$ 和$\odot_3$ 均不满足代换性质.

考察 ρ_d，有 $1\rho_d 1, a\rho_d 2, 1\rho_d 2, 2\rho_d 1, 0\rho_d 0$，容易验证 ρ_d 对于 $\odot_3$ 满足代换性质，但对于 $\oplus_3$ 不满足代换性质，因为 $2\rho_d' 0$，即 $(1\oplus_3 1)$ $\rho_d' (1\oplus_3 2)$. 于是此题的答案就出来了.

解 $\rho_d=\{(0,0),(1,1),(2,2),(1,2),(2,1)\}$ 是 Z_3 上的等价关系，它对于 $\odot_3$ 满足代换性质，对于 $\oplus_3$ 不满足代换性质.

例 B-2 给定代数系统 $V_1=\langle Z_2;\oplus_2\rangle$，$V_2=\langle Z_3;\oplus_3\rangle$ 和 $V_3=\langle Z_6;\oplus_6\rangle$，试证明 $V_1\times V_2$ 同构于 V_3.

分析 $V_1\times V_2=\langle Z_2\times Z_3;\oplus\rangle$，其中

$$Z_2\times Z_3=\{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2)\}$$

$$(x_1,y_1)\oplus(x_2,y_2)=(x_1\oplus_2 x_2, y_1\oplus_3 y_2).$$

这一代数系统的运算表列在表 4-3 中.

为了证明 $V_1\times V_2$ 同构于 V_3，我们需要恰当地定义一个函数 $h:Z_6\to Z_2\times Z_3$，使得 h 是双射且对于运算 $\oplus_6$ 和 $\oplus$ 满足同态的条件，即对于任意 $z_1,z_2\in Z_6$，有

$$h(z_1\oplus_6 z_2)=h(z_1)\oplus h(z_2).$$

证法一 定义函数 $h:Z_6\to Z_2\times Z_3$，使得对于任一 $z\in Z_6$，

$$h(z)=(\mathrm{res}_2(z),\mathrm{res}_2(z)).$$

由上面的定义我们得到 $h(0)=(0,0)$，$h(1)=(1,1)$，$h(2)=(0,2)$，$h(3)=(1,0)$，$h(4)=(0,1)$，$h(5)=(1,2)$，因此 h 是一个双射.

对于任意的 $z_1,z_2\in Z_6$，令 $z_1+z_2=6q+r\quad(0\leqslant r<6)$，则

$$\mathrm{res}_2(z_1+z_2)=\mathrm{res}_2(r),\mathrm{res}_3(z_1+z_2)=\mathrm{res}_3(r),$$

若令 $z_1=aq_1+r_1, z_2=aq_2+r_2(0\leqslant r_1,r_2<2)$，则

$$\mathrm{res}_2(z_1+z_2)=\mathrm{res}_2(r_1+r_2).$$

若令 $z_1=3p_1+i_1, z_2=3p_2+i_2(0\leqslant i_1,i_2<3)$，则

$$\mathrm{res}_3(z_1+z_2)=\mathrm{res}_3(i_1+i_2).$$

于是

$$\begin{aligned}h(z_1\oplus_6 z_2)&=h(\mathrm{res}_6(z_1+z_2))\\&=(\mathrm{res}_2(\mathrm{res}_6(z_1+z_2)),\mathrm{res}_3(\mathrm{res}_6(z_1+z_2)))\end{aligned}$$

$$= (\mathrm{res}_2(r), \mathrm{res}_3(r))$$
$$= (\mathrm{res}_2(z_1 + z_2), \mathrm{res}_3(z_1 + z_2)).$$
$$h(z_1) \oplus h(z_2) = (\mathrm{res}_2(z_1), \mathrm{res}_3(z_1)) \oplus (\mathrm{res}_2(z_2), \mathrm{res}_3(z_2))$$
$$= (\mathrm{res}_2(\mathrm{res}_2(z_1) + \mathrm{res}_2(z_2)), \mathrm{res}_3(\mathrm{res}_3(z_1) + \mathrm{res}_3(z_2)))$$
$$= (\mathrm{res}_2(r_1 + r_2), \mathrm{res}_3(i_1 + i_2))$$
$$= (\mathrm{res}_2(z_1 + z_2), \mathrm{res}_3(z_1 + z_2)).$$

因此

$$h(z_1 \oplus_6 z_2) = h(z_1) \oplus h(z_2).$$

故 h 是从 V_3 到 $V_1 \times V_2$ 的同构.

为了证明 $V_1 \times V_2$ 同构于 V_3，也可以通过恰当地定义一个函数 $f: Z_2 \times Z_3 \to Z_6$ 来实现. 同样地，需证明 f 是双射且对于任意的 $(a_1, b_1), (a_2, b_2) \in Z_2 \times Z_3$，有

$$f((a_1, b_1) \oplus (a_2, b_2)) = f(a_1, b_1) \oplus_6 f(a_2, b_2).$$

证法二 定义函数 $f: Z_2 \times Z_3 \to Z_6$，对于任意的 $(a, b) \in Z_2 \times Z_3$，有

$$f(a, b) = 3a \oplus_6 2b.$$

则 $h(0,0)=0, h(1,2)=3 \oplus_6 4=1, h(0,1)=0 \oplus_6 2=2,$
$h(1,0)=3 \oplus_6 0=3, h(0,2)=0 \oplus_6 4=4, h(1,1)=3 \oplus_6 2=5.$

显然 f 是双射.

对于任意 $(a_1, b_1), (a_2, b_2) \in Z_2 \times Z_3$，令

$$a_1 + a_2 = 2q_1 + r_1 \quad (0 \leqslant r_1 < 2),$$
$$b_1 + b_2 = 3q_2 + r_2 \quad (0 \leqslant r_2 < 3),$$

则

$$f((a_1, b_1) \oplus (a_2, b_2)) = f((a_1 \oplus_2 a_2), (b_1 \oplus_3 b_2))$$
$$= f(\mathrm{res}_2(a_1 + a_2), \mathrm{res}_3(b_1 + b_2))$$
$$= f(r_1, r_2) = 3r_1 \oplus_6 2r_2 = \mathrm{res}_6(3r_1 + 2r_2).$$

而

$$f(a_1,b_1) \oplus_6 f(a_2,b_2) = (3a_1 \oplus_6 2b_1) \oplus_6 (3a_2 \oplus_6 2b_2).$$

因为运算$\oplus_6$是可交换和可结合的，所以

$$\begin{aligned} f(a_1,b_1) \oplus_6 f(a_2,b_2) &= (3a_1 \oplus_6 3a_2) \oplus_6 (2b_1 \oplus_6 2b_2) \\ &= \mathrm{res}_6(3a_1 + 3a_2) \oplus_6 \mathrm{res}_6(2b_1 + 2b_2) \\ &= \mathrm{res}_6(3(aq_1 + r_1)) \oplus_6 \mathrm{res}_6(a(3q_2 + r_2)) \\ &= \mathrm{res}_6(3r_1) \oplus_6 \mathrm{res}_6(ar_2). \end{aligned}$$

因为 $0 \leqslant r_1 \leqslant 1$，所以 $0 \leqslant 3r_1 \leqslant 3$；因为 $0 \leqslant r_2 \leqslant 2$，所以 $0 \leqslant 2r_2 \leqslant 4$. 于是 $0 \leqslant 3r_1 < 6$，$0 \leqslant 2r_2 < 6$，因此

$$f(a_1,b_1) \oplus_6 f(a_2,b_2) = 3r_1 \oplus_6 2r_2 = \mathrm{res}_6(3r_1 + 2r_2),$$

$$f((a_1,b_1) \oplus (a_2,b_2)) = f(a_1,b_1) \oplus_6 f(a_2,b_2).$$

由上可知 f 是从 $V_1 \times V_2$ 到 V_3 的同态.

在例 5-46 中，我们曾证明了：凡阶等于 n 的有限循环群都相互同构.

另外，对于任意两个代数系统 $V_1 = \langle S_1; *_1 \rangle$ 和 $V_2 = \langle S_2; *_2 \rangle$，它们的积代数 $V_1 \times V_2 = \langle S_1 \times S_2; * \rangle$ 具有如下性质：若运算 $*_1$ 和 $*_2$ 是可结合的，则运算 $*$ 也是可结合的. 这一结论的证明很简单，读者自己可以完成.

利用上面这两条性质，我们又有第三种证明方法.

证法三 对于任意正整数 m，模 m 加法运算$\oplus_m$都是可结合的，因此 $V_1 \times V_2$ 中的$\oplus$和 V_3 中的$\oplus_6$都是可结合的. 又由$\oplus$和$\oplus_6$的运算表（参见表 4-3 和表 6-1）可知(0,0)和 0 分别是 $V_1 \times V_2$ 和 V_3 的单位元，在 $V_1 \times V_2$ 中(0,1)和(0,2)互为逆元，(1,0)以自身为逆元，(1,1)和(1,2)互为逆元，因此 $V_1 \times V_2$ 是一个群. 在 V_3 中 1 与 5 互为逆元，2 与 4 互为逆元，3 以自身为逆元，因此 V_3 也是一个群.

显然 1 是群 $\langle Z_6; \oplus_6 \rangle$ 的生成元. 又在 $V_1 \times V_2$ 中 $(1,1)^0 = (0,0)$ $(1,1)^1 = (1,1)$，$(1,1)^2 = (1,1) \oplus (1,1) = (0,2)$，$(1,1)^3 = (0,2) \oplus (1,1) = (1,0)$，$(1,1)^4 = (1,0) \oplus (1,1) = (0,1)$，$(1,1)^5 = (0,1) \oplus (1,1) = (1,2)$，因此 V_3 和 $V_1 \times V_2$ 都是阶为 6 的循环群.

由于阶为 n 的循环群都相互同构，故 $V_1 \times V_2$ 与 V_3 同构.

例 B-3 设 $\langle S; * \rangle$ 是一有限可交换的独异点，并且对于任意的 $a,b,c \in S$，由 $a*b=a*c$，可得 $b=c$. 试证明 $\langle S; * \rangle$ 是一交换群.

分析 独异点和群的区别在于，独异点中的元素不一定有逆元，而群中的每一个元素均有逆元. 此题实际上是要我们在 S 是有限的条件下由消去律推出可逆性.

证法一 令 $S=\{a_1,a_2,\cdots,a_n\}$，对任一元素 $a_i \in S(1 \leqslant i \leqslant n)$，考虑集合 $a_i * S=\{a_i*a_1,a_i*a_2,\cdots,a_i*a_n\}$，显然 $a_i * S \subseteq S$. 又由假设当 $a_j \neq a_k$ 时，$a_i*a_j \neq a_i*a_k$，因此 a_i*S 具有 n 个互不相同的元素，于是不得不有 $a_i*S=S$. 由此必存在元素 a_j，使得 $a_i*a_j=e$. 又由运算 $*$ 的可交换性，有 $a_i*a_j=a_j*a_i=e$，因此 a_i 有逆元. 由 a_i 的任意性，$\langle S; * \rangle$ 是一交换群.

参考文献[1]中证明了有限独异点的如下一条性质：设 $\langle S; * \rangle$ 是一有限独异点，则对每一 $a \in S$，存在一个整数 $j \geqslant 1$，使得 a^j 是一幂等元.

利用这一性质，我们可给出第二种证明方法.

证法二 因为 $\langle S; * \rangle$ 是一有限独异点，所以对于任一 $a \in S$，存在一正整数 j，使得 $a^j*a^j=a^j$，于是 $a^j*a^j=a^j*e$，由题设得 $a^j=e$. 因此

$$a^{j-1}*a=a*a^{j-1}=e \qquad (j-1 \geqslant 0).$$

这意味着 a^{j-1} 是 a 的逆元，由 a 的任意性，$\langle S; * \rangle$ 是一交换群.

证法三 设 $\#S=n$，则对于任一 $a \in S$，在序列 $a^0(=e),a,a^2,\cdots,a^n$ 中必有两个元素是相同的. 设 $a^i=a^j(0 \leqslant i<j \leqslant n)$，并令 $j=i+t(0<t \leqslant n)$，则

$$a^j=a^{i+t}=a^i*a^t=a^i=a^i*e$$

于是由题设 $a^t=e$，因此

$$a^{t-1}*a=a*a^{t-1}=e \qquad (t-1 \geqslant 0)$$

即 a^{t-1} 是 a 的逆元. 由 a 的任意性，$\langle S; * \rangle$ 是一交换群.

通过证明此题，读者应注意到以下两点：(1)无论用什么方法证明此题的结论，都必须用到“由 $a*b=a*c$，可得 $b=c$”这一条件. (2)虽然在证法一中用到了运算 $*$ 的可交换性，但从证法二和证法三中可以看出，运算 $*$ 的可交换性对于证明 $\langle S;*\rangle$ 的可逆性并不是必要的.

例 B-4 设 g 是由群 $\langle G;*\rangle$ 到群 $\langle G';\circ\rangle$ 的满同态，试证明若 $\langle N';\circ\rangle$ 是群 $\langle G';\circ\rangle$ 的正规子群，则 N' 的像源 N 对于运算 $*$ 也构成 $\langle G;*\rangle$ 的正规子群.

分析 ① $\langle N';\circ\rangle$ 是群 $\langle G';\circ\rangle$ 的正规子群，意味着对于任意的 $a'\in G'$，有 $a'\circ N'=N'\circ a'$ 或 $a'\circ N'\circ(a')^{-1}\subseteq N'$.

② N 是 N' 的象源意味着对于任意 $n\in N$，$g(n)\in N'$. 反之，对于每一个 $n'\in N'$，若 $g(n)=n'$，则 $n\in N$.

③要证明 N 与 $*$ 能构成 $\langle G;*\rangle$ 的正规子群，需要证明以下几点：

1)运算 $*$ 在 N 上封闭，即由 $n_1,n_2\in N$，可推出 $n_1*n_2\in N$；

2) $*$ 在 N 上可逆，即由 $n\in N$，可推出 $n^{-1}\in N$.

有了以上两条，$\langle N;*\rangle$ 便构成 $\langle G;*\rangle$ 的子群. 以上两条也可用一条来代替，即由 $n_1,n_2\in N$，推出 $n_1*n_2^{-1}\in N$.

3)对于任意 $a\in G$，$a*N*a^{-1}\subseteq N$.

证 因为 $\langle N';\circ\rangle$ 是 $\langle G';\circ\rangle$ 的子群，所以 $e'\in N'$，而 g 是满同态，$g(e)=e'$，所以 $e\in N$，N 非空.

设 $n_1,n_2\in N$，则必存在 $n_1',n_2'\in N'$，使得 $g(n_1)=n_1'$，$g(n_2)=n_2'$，由满同态的性质和 $\langle N';\circ\rangle$ 是 $\langle G';\circ\rangle$ 的子群，有

$$g(n_1*n_2^{-1})=g(n_1)\circ g(n_2^{-1})=g(n_1)\circ(g(n_2))^{-1}$$
$$=n_1'\circ(n_2')^{-1}\in N',$$

因此 $n_1*n_2^{-1}\in N$. 故 $\langle N;*\rangle$ 是 $\langle G;*\rangle$ 的子群.

对于任意的 $a\in G$ 和任意的 $n\in N$，有

$$g(a*n*a^{-1})=g(a)\circ g(n)\circ g(a^{-1})=a'\circ n'\circ(a')^{-1}$$

由于 $n'\in N'$，且 $\langle N';\circ\rangle$ 是 $\langle G';\circ\rangle$ 的正规子群，所以 $a'\circ n'\circ$

$(a')^{-1}\in N'$,即 $g(a*n*a^{-1})\in N'$. 因此 $a*n*a^{-1}\in N$. 由于 n 的任意性,$a*N*a^{-1}\subseteq N$. 故$\langle N;*\rangle$是$\langle G;*\rangle$的正规子群.

例 B-5 设$\langle G;*\rangle$是一个群,$R\subseteq G\times G$ 定义为

$$R=\{(a,b)\mid 存在 c\in G 使得 b=c*a*c^{-1}\},$$

试证明 R 是 G 上的等价关系.

分析 由题设 $R\subseteq G\times G$,所以 R 是 G 上的一个关系. 要证明 R 等价,需证明 R 具有自反性、对称性和可传递性.

证 设$\langle G;*\rangle$的单位元是 e,则对于任意的 $a\in G$,有 $a=e*a*e$,即 $a=e*a*e^{-1}$,于是有$(a,a)\in R$,R 是自反的.

设$(a,b)\in R$,则存在元素 $c\in G$,使得 $b=c*a*c^{-1}$,于是 $c^{-1}*b*c=c^{-1}*(c*a*c^{-1})*c$,因此 $a=c^{-1}*b*(c^{-1})^{-1}$,这说明$(b,a)\in R$,故 R 是对称的.

设(a,b)、$(b,c)\in R$,则存在元素 $h,d\in G$,使 $b=h*a*h^{-1}$,$c=d*b*d^{-1}$,于是

$$c=d*(h*a*h^{-1})*d^{-1}=(d*h)*a*(d*h)^{-1}.$$

这说明$(a,c)\in R$,故 R 是可传递的.

由上证得 R 是 G 上的等价关系.

例 B-6 设$\langle G;*\rangle$是一个 n 阶循环群,生成元为 a. 试证明对于 n 的任一因子 d,存在唯一的一个 d 阶子群.

分析 证明过程分为两个步骤:1)证明对于 n 的任一因子 d,存在$\langle G;*\rangle$的一个 d 阶子群;2)如果$\langle G;*\rangle$还有 d 阶子群,则必与 1)中的 d 阶子群是相同的.

证 因为$\langle G;*\rangle$是 n 阶循环群,所以生成元 a 的周期为 n,即 $a^n=e$,但 $a^i\neq e(0<i<n)$.

设 $n=dm$,则$(a^m)^d=e$,且对于任意正整数 t,若 $t<d$,则 $a^{mt}\neq e$. 因此元素 a^m 的周期为 d. 由于运算 $*$ 在$\{a^m,a^{2m},\cdots,a^{dm}(=e)\}$上是封闭的,因此$\langle\{a^m,a^{2m},\cdots,a^{dm}\};*\rangle$构成$\langle G;*\rangle$的阶为 d 的子群. 该子群是以 a^m 为生成元的循环群.

设$\langle H;*\rangle$也是$\langle G;*\rangle$的 d 阶子群,则由例 5-37 知$\langle H;*\rangle$是

一个循环群，令其生成元为 $a^s(s>0)$，则 a^s 的周期为 d(参阅参考文献[1]的定理 5-5)，即 $a^{sd}=e$ 且当 $0<k<d$ 时，$a^{sk}\neq e$，由 a 的周期为 n，必有 $sd=n$. 于是 $s=\frac{n}{d}=m$. 因此 $\langle H;*\rangle$ 是以 a^m 为生成元的 d 阶子群.

由上证得对于 n 的任一因子 d，$\langle G;*\rangle$ 必存在唯一的一个 d 阶子群.

例B-7 设 $G=\{f\mid f:R\to R$ 且 $f(x)=ax+b,a,b\in R,a\neq 0\}$。$\circ$ 是函数的复合运算(R 是实数集).

(1)证明 $\langle G;\circ\rangle$ 是一个群；

(2)G 的子集 S 和 T 分别定义如下：

$$S=\{f\mid f\in G \text{ 且 } f(x)=x+b\};$$
$$T=\{f\mid f\in G \text{ 且 } f(x)=ax\},$$

证明 $\langle S;\circ\rangle$ 和 $\langle T;\circ\rangle$ 都是 $\langle G;\circ\rangle$ 的子群；

(3)写出 $\langle S;\circ\rangle$ 和 $\langle T;\circ\rangle$ 在 $\langle G;\circ\rangle$ 中的所有左陪集.

分析 只要读者对群的定义、子群的判别方法及左陪集的概念清楚，完成此题并不困难. 关键是要熟悉题目所给的条件.

G 是由实数集 R 到 R 的其映射关系为 $f(x)=ax+b$ 的这类函数的集合，不是所有由 R 到 R 的函数的集合，这里 a 和 b 可以是任何实数，只要 $a\neq 0$。

S 是 G 中部分函数的集合，这些函数的共同特点是 a 取为 1，b 任意，由于 b 的取值有无穷多个，因此 S 中有无穷多个不同的函数.

T 也是 G 中部分函数的集合，这些函数的共同特点是 b 取为 0，a 是任意非零实数，由于 a 的取值可以不同，因此 T 中也有无穷多个不同的函数.

证 (1)设 $f_1,f_2\in G$ 且 $f_1(x)=a_1x+b_1$，$f_2(x)=a_2x+b_2$，$a_1\neq 0,a_2\neq 0$，则

$$f_1\circ f_2(x)=f_1(a_2x+b_2)=a_1(a_2x+b_2)+b_1$$

$$= a_1a_2x + (a_1b_2 + b_1)$$

$a_1a_2 \in R$ 且 $a_1a_2 \neq 0$，$a_1b_2 + b_1 \in R$.

因此 $f_1 \circ f_2 \in G$. 故 $\langle G; \circ \rangle$是一个代数系统

对于任意的 $f_1, f_2, f_3 \in G$，因为函数的复合运算是可结合的，所以有 $f_1 \circ (f_2 \circ f_3) = (f_1 \circ f_2) \circ f_3$.

令 $f_e: R—R$，使 $f_e(x) = x$，则对于任意 $f \in G$，设 $f(x) = ax + b$，有

$$f_e \circ f(x) = f_e(ax + b) = ax + b,$$

$$f \circ f_e(x) = f(x) = ax + b.$$

因此 $f_e \circ f = f \circ f_e \cdot f_e$ 是单位元.

对于任意的 $f \in G$，设 $f(x) = ax + b$，$a \neq 0$，存在函数 $g \in G$，$g(x) = \frac{1}{a}x - \frac{b}{a}$，使得

$$g \circ f(x) = g(ax + b) = \frac{1}{a}(ax + b) - \frac{b}{a} = x;$$

$$f \circ g(x) = f(\frac{1}{a}x - \frac{b}{a}) = a(\frac{1}{a}x - \frac{b}{a}) + b = x,$$

因此 $g \circ f = f \circ g = f_e$. 这说明任意 $f \in G$ 均存在逆元.

由上证得$\langle G; \circ \rangle$是一个群.

(2) 设 $f_1, f_2 \in S$，$f_1(x) = x + b_1$，$f_2(x) = x + b_2$，于是 $f_2^{-1}(x) = x - b_2$（f_2^{-1}表示 f_2 的逆元），并且

$$f_1 \circ f_2^{-1}(x) = f_1(x - b_2) = x - b_2 + b_1 = x + (b_1 - b_2) \in S.$$

因此$\langle S; \circ \rangle$是$\langle G; \circ \rangle$的子群.

设 $f_1, f_2 \in T$，$f_1(x) = a_1x$，$f_2(x) = a_2x$，$a_1 \neq 0$，$a_2 \neq 0$，于是 $f_2^{-1}(x) = \frac{1}{a_2}x$，并且

$$f_1 \circ f_2^{-1}(x) = f_1(\frac{1}{a_2}x) = a_1(\frac{1}{a_2}x) = \frac{a_1}{a_2}x, \frac{a_1}{a_2} \neq 0.$$

因此 $f_1 \circ f_2^{-1} \in T$. 故$\langle T; \circ \rangle$是$\langle G; \circ \rangle$的子群.

(3)对于任意一个函数 $h \in G$，设 $h(x) = cx + d$，则

$$h \circ S=\{h \circ f \mid f \in G, f(x)=x+b, b \in R\};$$

因为 $\quad h \circ f(x)=h(x+b)=c(x+b)+d=cx+(cb+d)$,

所以 $\quad h \circ S=\{\varphi \mid \varphi \in G, \varphi(x)=cx+(cb+d)\}$.

在集合 S 中,b 可为 R 中的任意实数,不同的 b 对应于不同的函数 f. 因此在集合 $h \circ S$ 中,对于给定的 c 和 d,$cb+d$ 可以为 R 中任意实数,不同的 $cb+d$ 对应不同的函数 φ,但集合 $h \circ S$ 中所有的函数具有共同的系数 c. 因此$\langle S; \circ \rangle$在$\langle G; \circ \rangle$中的所有左陪集为:对于每一个 $c \in R$,相应有$\langle S; \circ \rangle$的一个左陪集

$$\{\varphi \mid \varphi \in G, \varphi(x)=cx+b, b \in R\}.$$

对于任意一个函数 $h \in G$,设 $h(x)=cx+d$,则

$$h \circ T=\{h \circ f \mid f \in G, f(x)=ax, a \neq 0\},$$

因为 $\quad h \circ f(x)=h(ax)=cax+d$,

所以 $\quad h \circ T=\{\varphi \mid \varphi \in G, \varphi(x)=cax+d, ca \neq 0\}$.

在集合 T 中,a 可为任意非零实数,不同的 a 对应不同的函数 f. 因此在集合 $h \circ T$ 中对于给定的 c,d,ca 可为任意实数,不同的 ca 对应不同的 φ. 因此$\langle T; \circ \rangle$在$\langle G; \circ \rangle$中的所有左陪集为:对于每一个 $d \in R$,相应有$\langle T; \circ \rangle$的一个左陪集

$$\{\varphi \mid \varphi \in G, \varphi(x)=a'x+d, a' \in R\}.$$

例 B-8 设$\langle \{e, a_1, a_2, \cdots, a_{2n}\}; * \rangle$是一个交换群,$n$ 为正整数. 试证明 $a_1 * a_2 * \cdots * a_{2n}=e$

证 对任意元素 $a_i \in \{a_1, \cdots, a_{2n}\}$,设 a_i 的周期为 r_i,则 r_i 必是 $2n+1$ 的因子,从而 $r_i \neq 2$,即 $a_i^2 \neq e$,因此 $a_i^{-1} \neq a_i$. 故必有 $j \in \{1,2,\cdots,2n\}$,$j \neq i$,使 $a_j=a_i^{-1}$. 由群中元素逆元的唯一性和该群的可交换性知

$$a_1 * a_2 * \cdots * a_{2n}=(a_{k_1} * a_{k_1}^{-1}) * (a_{k_2} * a_{k_2}^{-1}) * \cdots * (a_{k_n} * a_{k_n}^{-1})=e.$$

例 B-9 设$\langle B; * \rangle$是群,$\langle A; \circ \rangle$是交换群,$F(B,A)=\{f \mid f: B \to A$ 是同态映射$\}$,对 $f, g \in F(B,A)$,定义 $f \oplus g$:对任意 $b \in B$,$f \oplus g(b)=f(b) \circ g(b)$. 试证明:

(1)$\oplus$是 $F(B,A)$上的二元运算;

(2)$\langle F(B,A);\oplus\rangle$是交换群；

(3)对于整数加群$\langle I;+\rangle$，$\langle F(I,A);\oplus\rangle$与$\langle A;\circ\rangle$同构.

证 (1)根据$\oplus$的定义，对任意的$f,g\in F(B,A)$，对任意的$b\in B$

$$(f\oplus g)(b)=f(b)\circ g(b)\in B,$$

所以$f\oplus g$是由B到A的函数.

对于任意的$b_1,b_2\in B$，因为f和g都是同态且运算$\circ$是可交换的，所以

$$\begin{aligned}(f\oplus g)(b_1*b_2)&=f(b_1*b_2)\circ g(b_1*b_2)\\&=f(b_1)\circ f(b_2)\circ g(b_1)\circ g(b_2)\\&=(f(b_1)\circ g(b_1))\circ(f(b_2)\circ g(b_2))\\&=(f\oplus g)(b_1)\circ(f\oplus g)(b_2).\end{aligned}$$

因此$f\oplus g$是同态映射. 故$\oplus$是$F(B,A)$上的二元运算.

(2)对任意$f,g,h\in F(B,A)$和任意的$b\in B$，有

$$\begin{aligned}((f\oplus g)\oplus h)(b)&=(f\oplus g)(b)\circ h(b)\\&=(f(b)\circ g(b))\circ h(b)\\&=f(b)\circ(g(b)\circ h(b))\\&=f(b)\circ g\oplus h(b)\\&=f\oplus(g\oplus h)(b),\end{aligned}$$

所以 $(f\oplus g)\oplus h=f\oplus(g\oplus h)$.

对任意$f,g\in F(B,A)$和任意$b\in B$，

$$f\oplus g(b)=f(b)\circ g(b)=g(b)\circ f(b)=(g\oplus f)(b),$$

所以 $f\oplus g=g\oplus f$.

定义函数$f_e:B\to A$，使得对于任意$b\in B$，$f_e(b)=e_A$(e_A表示$\langle A;\circ\rangle$的单位元). 显然f_e是同态映射，且对于任意的f和任意的$b\in B$，

$$(f_e\oplus f)(b)=f_e(b)\circ f(b)=e_A\circ f(b)=f(b)$$

类似地 $(f\oplus f_e)(b)=f(b)\circ e_A=f(b)$，因此$f_e$是$\langle F(B,A);\oplus\rangle$的单位元.

对任意 $f\in F(B,A)$，定义函数 $f^{-1}:B\to A$，使对于任意的 $b\in B$，$f^{-1}(b)=(f(b))^{-1}$. 于是对于任意的 $b_1,b_2\in B$，有

$$
\begin{aligned}
f^{-1}(b_1*b_2)&=(f(b_1*b_2))^{-1}=(f(b_1)\circ f(b_2))^{-1}\\
&=(f(b_2)\circ f(b_1))^{-1}=(f(b_1))^{-1}\circ(f(b_2))^{-1}\\
&=f^{-1}(b_1)\circ f^{-1}(b_2)
\end{aligned}
$$

因此 f^{-1}是同态映射且对于任意的 $b\in B$，有

$$(f\oplus f^{-1})(b)=f(b)\circ f^{-1}(b)=f(b)\circ(f(b))^{-1}=e_A=f_e(b).$$

因为运算$\oplus$可交换，所以 f^{-1}是 f 的逆元.

由上证得$\langle F(B,A);\oplus\rangle$是交换群.

(3)对任一 $f\in F(I,A)$，因为 f 是同态，由例 5-15 知 $f(0)=e_A$，又设 $f(1)=a$，则对于任意正整数 n，

$$f(n)=f(1+1+\cdots+1)=f(1)\circ f(1)\circ\cdots\circ f(1)=a^n;$$

$$
\begin{aligned}
f(-n)&=f((-1)+(-1)+\cdots+(-1))\\
&=f(-1)\circ f(-1)\circ\cdots\circ f(-1)\\
&=(a^{-1})^n=a^{-n}.
\end{aligned}
$$

所以对于任意整数 n，$f(n)=a^n$. 于是对任意的 $f,g\in F(I,A)$，若 $f(1)=g(1)=a$，则 $f=g$. 若 $f(1)=a$，则记 f 为 f_a.

定义函数 $\varphi:F(I,A)\to A$，对任意 $f_a\in F(I,A)$，$\varphi(f_a)=a$. 显然 φ是一个双射.

对于任意的 $f_a,f_b\in F(I,A)$，有

$$(f_a\oplus f_b)(1)=f_a(1)\circ f_b(1)=a\circ b=f_{a\circ b}(1),$$

$$\varphi(f_a\oplus f_b)=\varphi(f_{a\circ b})=a\circ b.$$

又　$\varphi(f_a)\circ\varphi(f_b)=a\circ b$，因此

$$\varphi(f_a\oplus f_b)=\varphi(f_a)\circ\varphi(f_b).$$

由上证得$\langle F(I,A);\oplus\rangle$与$\langle A;\circ\rangle$同构.

例 B-10　设$\langle H_1;*\rangle$和$\langle H_2;*\rangle$是群$\langle G;*\rangle$的两个互不包含的子群。试证明 G 中至少有一个元素 $g\in G$，使 $g\notin H_1\cup H_2$.

证　因为 $H_1\not\subseteq H_2$，所以必存在元素 $a\in H_1$，但 $a\notin H_2$；因为

$H_2 \not\subseteq H_1$，所以必存在元素 $b \in H_2$，但 $b \notin H_1$.

令元素 $a * b = d$，若 $d \in H_1$，则 $b = a^{-1} * d \in H_1$，与 $b \notin H_1$ 相矛盾；若 $d \in H_2$，则 $a = d * b^{-1} \in H_2$，与 $a \notin H_2$ 相矛盾. 因此 $a * b \notin H_1$ 且 $a * b \notin H_2$，故 $a * b \notin H_1 \cup H_2$.

例 B-11 设 $A = \{1,2,3\}, B = \{0,1\}, F = \{f \mid f: A \to B\}$

(1)列出集合 F 的全部元素；

(2)令 $G = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$，即 G 是 A 上三个置换组成的集合. 在 F 上定义关系 ρ，使得对于任意的 $f_i, f_j \in F$，当且仅当存在 $\varphi \in G$，使 $f_i = f_j \circ \varphi$ 时，$f_i \rho f_j$. 这里 $\circ$ 表示函数的复合运算. 试证明 ρ 是 F 上的等价关系.

(3)求出 F 关于 ρ 的商集 F/ρ.

解 (1)因为 $\# A = 3, \# B = 2$，所以 $\# F = 2^3 = 8$. 即 F 有 8 个元素，它们是

$$f_1: A \to B, f_1(1) = f_1(2) = f_1(3) = 0;$$
$$f_2: A \to B, f_2(1) = f_2(2) = f_2(3) = 1;$$
$$f_3: A \to B, f_3(1) = 0, f_3(2) = f_3(3) = 1;$$
$$f_4: A \to B, f_4(1) = 1, f_4(2) = f_4(3) = 0;$$
$$f_5: A \to B, f_5(2) = 0, f_5(1) = f_5(3) = 1;$$
$$f_6: A \to B, f_6(2) = 1, f_6(1) = f_6(3) = 0;$$
$$f_7: A \to B, f_7(3) = 0, f_7(1) = f_7(2) = 1;$$
$$f_8: A \to B, f_8(3) = 1, f_8(1) = f_8(2) = 0.$$

(2)证明 $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ 是集合 A 上的恒等函数，用 I_A 表示. 令 $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$. 容易验证函数的复合运算在 G 上是封闭的. 又 α 与 β 均是双射且互为逆函数. 即 $\alpha^{-1} = \beta, \beta^{-1} = \alpha, I_A^{-1} = I_A$.

对任意的 $f_i \in F$，有 $f_i = f_i \circ I_A$，即 $f_i \rho f_i$. 所以 ρ 是自反的.

若 $f_i \rho f_j$，则存在 $\varphi \in G$，使得 $f_i = f_j \circ \varphi$. 于是 $f_i \circ \varphi^{-1} = (f_j \circ$

$\varphi)\circ\varphi^{-1}$，$f_i\circ\varphi^{-1}=f_j$ 因此 $f_j\rho f_i$，故 ρ 是对称的.

若 $f_i\rho f_j$，$f_j\rho f_k$，则存在 $\varphi_1,\varphi_2\in G$，使得 $f_i=f_j\circ\varphi_1$，$f_j=f_k\circ\varphi_2$，于是

$$f_i=(f_k\circ\varphi_2)\circ\varphi_1=f_k\circ(\varphi_2\circ\varphi_1)=f_k\circ\varphi.\quad \varphi\in G$$

因此 $f_i\rho f_k$. 故 ρ 是可传递的.

由上证得 ρ 是 F 上的等价关系.

(3) 显然，对任意的 $\varphi\in G$，均有 $f_1=f_1\circ\varphi$，$f_2=f_2\circ\varphi$.

对于 f_3，有 $f_3=f_3\circ I_A$，$f_7=f_3\circ\alpha$，$f_5=f_3\circ\beta$，

对于 f_4，有 $f_4=f_4\circ I_A$，$f_8=f_4\circ\alpha$，$f_6=f_4\circ\beta$.

根据 ρ 的自反性、对称性和可传递性，得到 ρ 的以下等价类：$\{f_1\}$，$\{f_2\}$，$\{f_3,f_5,f_7\}$，$\{f_4,f_6,f_8\}$. 因此商集

$$F/\rho=\{\{f_1\},\{f_2\},\{f_3,f_5,f_7\},\{f_4,f_6,f_8\}\}.$$

例 B-12 设 $\langle L;\leqslant_1\rangle$ 和 $\langle S;\leqslant_2\rangle$ 是两个格，f 是 L 到 S 的双射. 证明 f 是同构映射的充要条件为对 $\forall\ a,b\in L$，有 $a\leqslant_1 b\Longleftrightarrow f(a)\leqslant_2 f(b)$.

证 设对应于格 $\langle L;\leqslant_1\rangle$ 和 $\langle S;\leqslant_2\rangle$ 的代数系统形式分别为 $\langle L;\vee,\wedge\rangle$ 和 $\langle S;\oplus,\otimes\rangle$.

必要性 设 f 是同构映射.

对 $\forall\ a,b\in L$，若 $a\leqslant_1 b$，则由定理 7.3.1 知 $a\wedge b=a$，而 f 是同态映射，所以 $f(a)=f(a\wedge b)=f(a)\otimes f(b)$，于是 $f(a)\leqslant_2 f(b)$.

另一方面，若 $f(a)\leqslant_2 f(b)$，则由定理 7.3.1 和 f 的同态性得 $f(a)=f(a)\otimes f(b)=f(a\wedge b)$.

而 f 是内射，所以 $a=a\wedge b$，从而 $a\leqslant_1 b$，因此有

$$a\leqslant_1 b\Longleftrightarrow f(a)\leqslant_2 f(b)$$

充分性 因为 f 是双射，所以只需证 f 是同态映射.

对 $\forall\ a,b\in L$，因为 $a\wedge b\leqslant_1 a$，$a\wedge b\leqslant_1 b$. 所以，由条件知 $f(a\wedge b)\leqslant_2 f(a)$，$f(a\wedge b)\leqslant_2 f(b)$.

根据定理 7.4.1 及等幂律得

$$f(a\wedge b)=f(a\wedge b)\otimes f(a\wedge b)\leqslant_2 f(a)\otimes f(b),$$

$$f(a \wedge b) \leqslant_2 f(a) \otimes f(b). \qquad (1)$$

另一方面，因为 $f(a)\otimes f(b)\in S$ 且 f 是双射，所以，存在 $c\in L$，使 $f(c)=f(a)\otimes f(b)$，而 $f(c)=f(a)\otimes f(b)\leqslant_2 f(a)$，即 $f(c)\leqslant_2 f(a)$，类似 $f(c)\leqslant_2 f(b)$.

由条件可得 $c\leqslant_1 a, c\leqslant_1 b$，所以 $c\leqslant_1 a\wedge b$.于是 $f(c)\leqslant_2 f(a\wedge b)$，即

$$f(a) \otimes f(b) \leqslant f(a \wedge b) \qquad (2)$$

因此，由(1)，(2)得 $f(a\wedge b)=f(a)\otimes f(b)$. 类似可证 $f(a\vee b)=f(a)\oplus f(b)$.

从而 f 是同态映射，所以 f 是同构映射.

例 B-13 设 $\langle B;-,\vee,\wedge\rangle$ 是一布尔代数，试证明 $\langle B;\oplus\rangle$ 是一交换群，这里 $\oplus$ 定义为

$$a \oplus b = (a \wedge \bar{b}) \vee (\bar{a} \wedge b).$$

证 因为 $\langle B;-,\vee,\wedge\rangle$ 是一布尔代数，所以对 $\forall\, a,b\in L$，显然 $(a\wedge\bar{b})\vee(\bar{a}\wedge b)\in B$，故 $\oplus$ 在 B 上封闭. 下面证 $\oplus$ 满足结合律，交换律，在 B 上有单位元，且 B 中任意元素可逆.

(1)对 $\forall\, a,b,c\in B$，有

$$\begin{aligned}
(a \oplus b) \oplus c &= ((a \wedge \bar{b}) \vee (\bar{a} \wedge b)) \oplus c \\
&= [((a \wedge \bar{b}) \vee (\bar{a} \wedge b)) \wedge \bar{c}] \\
&\quad \vee [(\overline{(a \wedge \bar{b}) \vee (\bar{a} \wedge b)}) \wedge c] \\
&= (a \wedge \bar{b} \wedge \bar{c}) \vee (\bar{a} \wedge b \wedge \bar{c}) \\
&\quad \vee [((\bar{a} \vee b) \wedge (a \vee \bar{b})) \wedge c] \\
&= (a \wedge \bar{b} \wedge \bar{c}) \vee (\bar{a} \wedge b \wedge \bar{c}) \\
&\quad \vee [((\bar{a} \wedge \bar{b}) \vee (a \wedge b)) \wedge c] \qquad (\text{例 } 7\text{-}21) \\
&= (a \wedge \bar{b} \wedge \bar{c}) \vee (\bar{a} \wedge b \wedge \bar{c}) \\
&\quad \vee (\bar{a} \wedge \bar{b} \wedge c) \vee (a \wedge b \wedge c).
\end{aligned}$$

$$a \oplus (b \oplus c) = a \oplus ((b \wedge \bar{c}) \vee (\bar{b} \wedge c))$$

$$= a \wedge [\overline{(b \wedge \bar{c}) \vee (\bar{b} \wedge c)}] \vee [\bar{a} \wedge ((b \wedge \bar{c}) \vee (\bar{b} \wedge c))]$$

$= [a \wedge ((\bar{b} \vee c) \wedge (b \vee \bar{c}))] \vee [(\bar{a} \wedge b \wedge \bar{c}) \vee (\bar{a} \wedge \bar{b} \wedge c)]$

$= [a \wedge ((\bar{b} \wedge \bar{c}) \vee (b \wedge c))] \vee (\bar{a} \wedge b \wedge \bar{c}) \vee (\bar{a} \wedge \bar{b} \wedge c)$

（由例 7-21）

$= (a \wedge \bar{b} \wedge \bar{c}) \vee (a \wedge b \wedge c) \vee (\bar{a} \wedge b \wedge \bar{c}) \vee (\bar{a} \wedge \bar{b} \wedge c)$，

所以$(a \oplus b) \oplus c = a \oplus (b \oplus c)$　结合律成立.

(2)因为$a \oplus b = (a \wedge \bar{b}) \vee (\bar{a} \wedge b) = (b \wedge \bar{a}) \vee (\bar{b} \wedge a) = b \oplus a$ 所以交换律成立.

(3)对$\forall\ a \in B$，有

$$a \oplus 0 = (a \wedge \bar{0}) \vee (\bar{a} \wedge 0) = (a \wedge 1) \vee (\bar{a} \wedge 0)$$
$$= a \wedge 1 = a.$$

类似地有　$0 \oplus a = a$，所以 0 是 B 上关于$\oplus$的单位元.

(4)因为　$a \oplus a = (a \wedge \bar{a}) \vee (\bar{a} \wedge a) = 0 \vee 0 = 0$，所以

$$a^{-1} = a,$$

因此$\langle B;\oplus \rangle$是一交换群.

第三部分　图　论

第八章　图　论

8.1　内容提要

1. 图的基本概念

• 图，n 阶图，(n,m)图、无向图，有向图，伪图，多重图，简单图；

• 边关联结点，结点关联边，结点的邻接，边的邻接，孤立点，孤立边；

• 完全图，补图，结点的度数，正则图；

• 子图，真子图，生成子图；图的同构.

2. 图中的边数分别与结点度数、结点个数间的关系

• 握手定理：在(n,m)图中，$\sum_{i=1}^{n}\deg(v_i)=2m$；

• n 阶完全图 K_n 中，$m=\frac{1}{2}n(n-1)$

3. 路

• 开路，回路，真路，环路，链，闭链；

• 结点间的连接，连通图，连通子图，分图；

• 短程，距离（n 阶图中，$d(v_i,v_j)\leqslant(n-1)$）；

• 有向图的弱连通，单向连通，强连通.

4. 图的矩阵表示

- 邻接矩阵 A；
- 连接矩阵 C.

5. 图的连通性

- 割边，割点，边割集，点割集，断集；
- G 的连通度 $K(G)$，G 的边连通度 $\lambda(G)$，G 的最小度 $\delta(G)$.
- 点的连通度，边的连通度以及最小度间的关系.

$$K(G)\leqslant\lambda(G)\leqslant\delta(G).$$

6. 欧拉图和哈密顿图

- 欧拉图，欧拉回路，欧拉路
- 欧拉定理；
- 哈密顿环，哈密顿图，哈密顿路，闭图，闭包；
- 哈密顿图的判定条件，最邻近方法.

7. 树

- 树，树林，树叶；
- 树的性质及判定条件；
- 生成树，最小生成树.

8. 有向树

- 根，分枝结点，叶结点，级，子树；
- m 元树，完全 m 元树，二元树，完全二元树；
- 树的扫描.

9. 二部图

- 二部图 $G=(V_1,V_2,E)$，完全二部图 $K_{m,n}$；

- V_1 对 V_2 的匹配；
- 相异性条件；
- t-条件.

10. 平面图

- 平面图，面，边界，有限面，无限面，面的相邻；
- 欧拉公式；
- Kuratowski 定理.

8.2 基本知识点

1. 图的基本述语

无向图：一个无向图 G 是一个有序二元组 (V,E)，记作 $G=(V,E)$. 其中 V 是一有限非空集合，E 是 V 中不同元素的非有序对偶（即形如 $\{v_i,v_j\}$，$v_i\neq v_j$）的集合. 分别称 V 和 E 是图 G 的结点集合和边集合. V 中的元素是图 G 的结点（或顶点），E 中的元素是图 G 的边，记作 $e=\{v_i,v_j\}$，称 v_i,v_j 为 e 的端点.

在无向图 $G=(V,E)$ 中，若 E 是 V 中任意元素的非有序对偶的多重集（即元素可重复出现的集合），则称 G 是一个伪图. 没有自环（即 $\forall\ v_i\in V$，$\{v_i,v_i\}\notin E$）的伪图称为多重图. 没有自环且没有重数大于 1 的边的图称为简单图. 这样，我们前面所定义的无向图就是简单图，这点与其他书上的定义有所不同，请读者注意区别.

例 8-1 设 $G=(V,E)$ 是一无向图，$V=\{v_1,v_2,\cdots,v_8\}$，$E=\{\{v_1,v_2\},\{v_2,v_3\},\{v_3,v_1\},\{v_1,v_5\},\{v_5,v_4\},\{v_4,v_3\},\{v_7,v_8\}\}$.

(1)画出 G 的图解；

(2)指出与 v_3 邻接的结点，以及和 V_3 关联的边；

(3)指出与 e_1 邻接的边和与 e_1 关联的结点；

(4)该图是否有孤立结点和孤立边？

(5)求出各结点的度数,并判断是否是完全图和正则图;

(6)该(n,m)图中,$n=?$,$m=?$

解 (1)所给图 G 的一个图解如图 8-1 所示;

图 8-1

(2)v_1,v_2,v_4 均与 v_3 邻接,v_3 关联边 e_1,e_2,e_3;

(3)边 e_2,e_3,e_4 均与 e_1 邻接,e_1 关联结点 v_2,v_3;

(4)v_6 是孤立结点,e_5 是孤立边;

(5)$\deg(v_1)=3,\deg(v_2)=2,\deg(v_3)=3,\deg(v_4)=2,\deg(v_5)=2,\deg(v_6)=0,\deg(v_7)=1,\deg(v_8)=1$.

因为不是所有结点的度数均相等,故不是正则图,又 v_6 不与任何结点邻接,因此,G 也不是完全图.

(6)G 是(8,7)图或 8 阶图,$n=8$ 个结点,$m=7$ 条边.

例 8-2 图 8-2 给出了无向图 $G_1=(V_1,E_1)$和 $G_2=(V_2,E_2)$,它们各是什么类型的图,求出 G_1 的最大度数 $\Delta(G_1)$和最小度数 $\delta(G_1)$,并指出 G_1 中重数大于 1 的边.

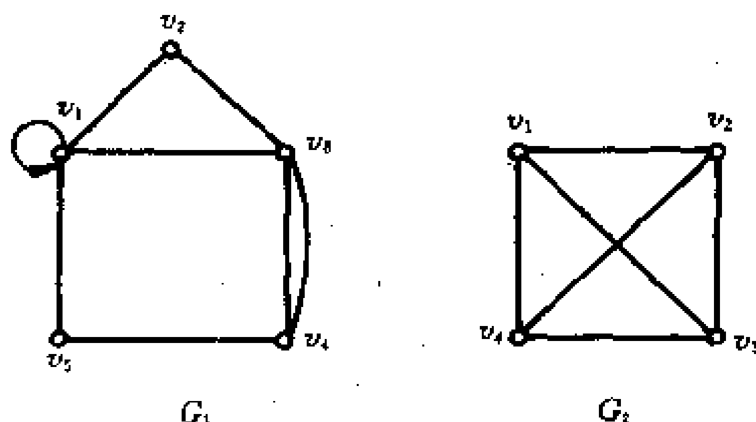


图 8-2

解 G_1 是一个伪图，有自环$\{v_1,v_1\}$和平行边$\{v_3,v_4\}$，$\{v_3,v_4\}$. G_2 是一个简单图，且 G_2 中任意两个结点均邻接，故是完全图，又每个结点的度数为 3，因此 G_2 是 3 次正则图.

G_1 中关联于 v_1 的结点的边有一个是自环，在计算 v_1 的度数时，此边使 v_1 的度增加 2，于是 $\deg(v_1)=5$，因此 $\Delta(G_1)=\max\{\deg(v)\mid v\in V_1\}=5$，$\delta(G_1)=\min\{\deg(v)\mid v\in V_1\}=2$.

G_1 中结点 v_3 与 v_4 间有两条平行边，边的重数为 2.

例 8-3 求图 G（如图 8-3 所示）的补图 $\overline{G}$.

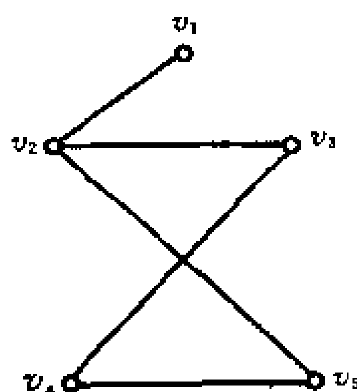


图 8-3

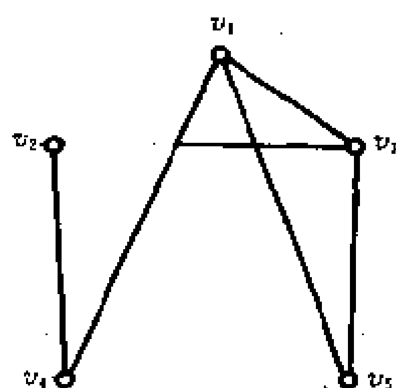


图 8-4

解 G 的补图 $\overline{G}$，是由 G 的所有结点和为了使 G 成为完全图所需要添加那些边组成的图，如图 8-4 所示.

例 8-4 图 8-5 给出了图 G_1,G_2,G_3,G_4，问它们之间有何关系？

解 $G_1=(V_1,E_1)$是一个 3 次正则图；因为 $V_3\subseteq V_1$ 且 $E_3\subset E_1$，所以 $G_3=(V_3,E_3)$是 G_1 的一个真子图；

又因为 $V_4=V_1$ 且 $E_4\subseteq E_1$，故所以 $G_4=(V_4,E_4)$是 G_1 的一个生成子图.

设 $G_2=(V_2,E_2)$ 因为$\{v_3,v_5\}\in E_2$，但$\{v_3,v_5\}\notin E_1$，

所以 $E_2\nsubseteq E_1$

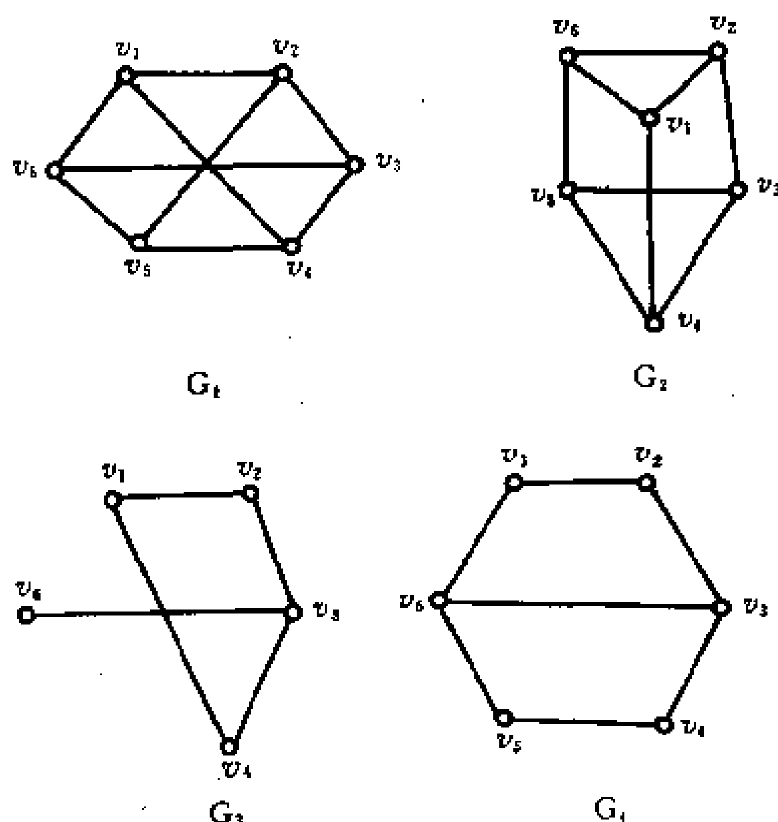


图 8-5

另一方面$\{v_3,v_6\}\in E_1$，但$\{v_3,v_4\}\notin E_2$，$\therefore E_1 \nsubseteq E_2$. 因此，$G_2$ 不是 G_1 的子图，G_1 也不是 G_2 的子图，同理 G_3，G_4 与 G_2 也没有子图关系.

例 8-5 设 G 是具有 3 个结点的完全图，试问：

(1)G 有多少个子图?

(2)G 有多少个生成子图?

(3)如果没有任何两个子图是同构的，则 G 的子图个数是多少? 将这些构造出来.

解 (1)$\because$含有一个结点的子图有 $C_3^1=3$ 个；

含二个结点的子图有 $C_3^2\cdot 2=6$；

含三个结点的子图有 $C_3^3\cdot 2^3=8$；

所以 G 共有 3+6+8=17 个子图.

(2)G 的生成子图，含 G 的全部结点，因为 G 有三条边，构成子图时，每条边有被选和不选两种情况.

所以 G 的生成子图的个数为 $2^3=8$.

(3)G 的所有不同构的子图如图 8-6 所示.

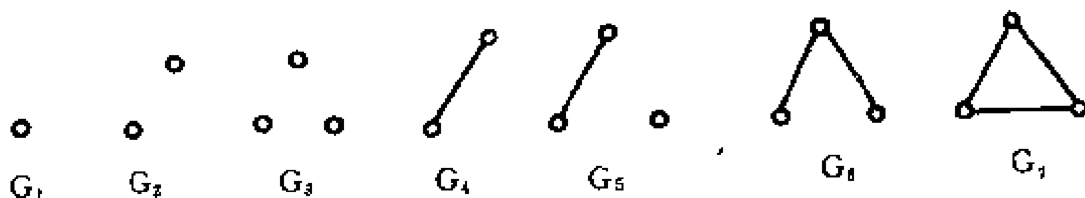


图 8-6

2. 图的同构

设有图 $G=(V,E)$和 $G'=(V',E')$，若存在双射 $h:V\to V'$使得边之间有如下关系：

$$e=\{v_i,v_j\}\in E \text{ iff } e'=\{h(v_i),h(v_j)\}\in E' \qquad (*)$$

则 G'同构于 G，或称 G 和 G'同构. 记作 $G\cong G'$.

由同构的定义可知，两个图同构的必要条件是：

(1)它们有相同的结点数和相同的边数；

(2)对应结点的度数相同. (即 $\deg(v_i)=\deg(h(v_i))$)

例 8-6 图 8-7 所示图 G_1 与 G_2 是否同构？

G_3 与 G_4 是否同构？

解 $\#V_1=\#V_2=6$，$\#E_1=\#E_2=9$.

根据点与边的关联关系，构造 $h:V_1\to V_2$，$h(v_i)=u_i(i=1,2,3,4)$，$h(v_5)=u_6$，$h(v_6)=u_5$. 显然 h 是双射，且满足图的同构定义中条件(*)，故是使 $G_1\cong G_2$ 的同构映射.

G_3 与 G_4 不同构.

假定 $G_3\cong G_4$，则存在 $h:V_3\to V_4$ 是双射，且满足(*). $h(v_1)=u_1$ 或者 $u_2\cdots$或者 u_6.

不妨设 $h(v_1)=u_1$，因$\{v_1,v_3\}$，$\{v_1,v_4\}$，$\{v_1,v_2\}\in E_3$.

所以$\{u_1,h(v_3)\}$，$\{u_1,h(v_4)\}$，$\{u_1,h(v_2)\}\in E_4$.

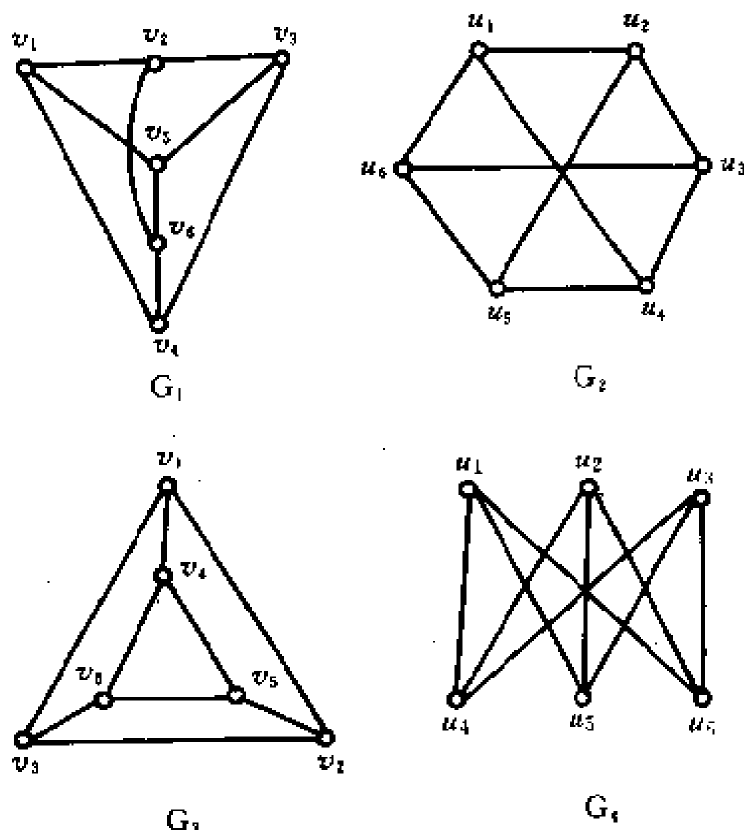


图 8-7

因此只有 $h(v_3)=u_4$ 或 u_5 或 u_6，$h(v_4)=u_4$ 或 u_5 或 u_6，$h(v_2)=u_4$ 或 u_5 或 u_6.

但 $\{v_3,v_2\}\in E_3$，而 u_4,u_5,u_6 间没有一对结点邻接，这与 h 满足(*)矛盾，故假设错误，G_3 与 G_4 不同构.

3. 结点的度数与边间的关系

握手定理　设 $G=(V,E)$ 是一个 (n,m) 图，则 $\sum_{i=1}^{n}\deg(v_i)=2m$.

在一个 n 阶完全图 G 中，边数 m 与结点数 n 满足　$m=C_n^2=\frac{1}{2}n(n-1)$.

例 8-7　设 $G=(V,E)$ 有 12 条边，有 6 个度为 3 的结点，其余

结点的度数均小于 3. 问 G 中至少有多少个结点？说明理由.

解 设 G 中有 n 个结点，由握手定理知

$$\sum_{i=1}^{n}\deg(v_i)=2m=24.$$

由条件可得 $24<6\times3+3\times(n-6)$，

$\therefore 3n>24, n>8.$

因此，G 中至少有 9 个结点.

例8-8 设(n,m)图$G=(V,E)$是简单图，则$\delta(G)\leqslant\frac{2m}{n}\leqslant\Delta(G)$.

证 对 G 中任意结点 v，由最大度和最小度的定义知 $\delta(G)\leqslant\deg(v)\leqslant\Delta(G)$.

又由握手定理 $\sum_{i=1}^{n}\deg(v_i)=2m$ 得

$$n\cdot\delta(G)\leqslant\sum_{i=1}^{n}\deg(v_i)\leqslant n\cdot\Delta(G),$$

$$n\cdot\delta(G)\leqslant 2m\leqslant n\cdot\Delta(G),$$

$$\therefore \quad \delta(G)\leqslant 2m/n\leqslant\Delta(G).$$

4. 路与回路

例 8-9 给定图 $G=(V,E)$如图 8-8 所示，

(1)在 G 中找一条长为 7 的开路且不是真路；

(2)在 G 中找一条长为 6 的回路且不是环路；

(3)在 G 中找一条长为 7 的真路；

(4)在 G 中找一个长为 5 的环路；

(5)在 G 中找一条长为 5 的链，且不是真路；

(6)在 G 中找一个长为 6 的闭链，

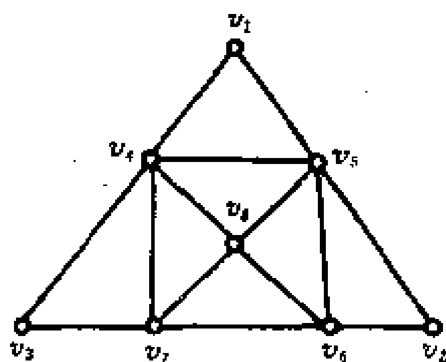


图 8-8

且不是环路；

(7)求出 v_2 与 v_3 的距离 $d(v_2,v_3)$.

解 (1)L_1：$v_4v_3v_7v_4v_1v_5v_6v_8$ (因 v_4 出现二次，故不是真路.)；

(2)L_2：$v_4v_5v_2v_6v_5v_8v_4$(因为 v_5 出现二次，所以不是环路)；

(3)L_3：$v_1v_5v_2v_6v_8v_4v_3v_7$；

(4)L_4：$v_4v_5v_6v_8v_7v_4$；

(5)L_5：$v_4v_3v_7v_4v_1v_5$(因 v_4 出现二次，故不是真路，但边未重复，故是链)；

(6)L_6：$v_4v_5v_2v_6v_5v_8v_4$(因 v_5 出现二次，故不是环路)；

(7)v_2 到 v_3 的路很多，其中长度最短的真路称为 v_2 到 v_3 的短程 L，其长度称为 v_2 到 v_3 的距离. 如 L_7：$v_2v_5v_4v_3$，L_8：$v_2v_6v_7v_3$ 均是 v_2 到 v_3 的短程，$d(v_2,v_3)=3$.

注 两个结点间的短程不唯一，但距离唯一.

5. 连通图和分图

在图 G 中，若存在一条路连接 v_i 和 v_j，则称结点 v_i 与 v_j 是连接的，若 G 中任意两个结点均是连接的，则称图 G 是连通的，否则 G 是不连通的.

图 G 的极大连通子图称为 G 的分图. 所谓 G 的极大连通子图 H 是指，H 是 G 的一个子图且 H 是连通的，而 G 的任何包含 H 的其他子图均不是连通的.

值得注意的是，图 G 的每个分图是连通的，若 G 只有一个分图，那么 G 是连通图.

定理 8.5.1 在 n 阶图 $G=(V,E)$ 中，若两个不同结点 u，v 间有一条路，则 u 到 v 间一定有一条长度不大于 $n-1$ 的真路.

例 8-10 给定图 $G=(V,E)$ 如图 8-9 所示，问 $H_1=(V_1,E_1)$，$H_2=(V_2,E_2)$，$H_3=(V_3,E_3)$ 是否是 G 的分图？其中

$$V_1=\{v_1,v_2,v_3,v_6\}；$$

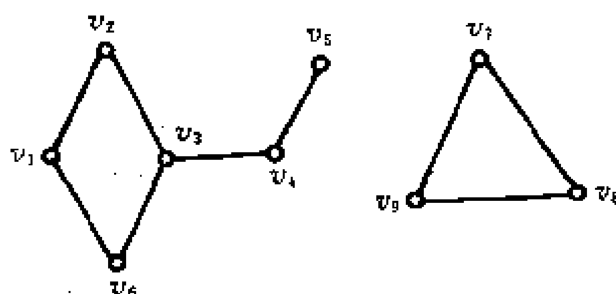
$$E_1 = \{\{v_1, v_2\}, \{v_2, v_3\}, \{v_3, v_6\}, \{v_6, v_1\}\};$$

$$V_2 = \{v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8\};$$

$$E_2 = \{\{v_1, v_2\}, \{v_2, v_3\}, \{v_3, v_6\}, \{v_6, v_1\}, \{v_3, v_4\}, \{v_4, v_5\}, \{v_7, v_8\}\};$$

$$V_3 = \{v_1, v_2, v_3, v_4, v_5, v_6\};$$

$$E_3 = \{\{v_1, v_2\}, \{v_2, v_3\}, \{v_3, v_6\}, \{v_6, v_1\}, \{v_3, v_4\}, \{v_4, v_5\}\}.$$



G

图 8-9

解 H_1 是 G 的连通子图，但 $H_1'=(V_1', E_1')$ 包含 H_1 且也是 G 的连通子图. 所以 H_1 不是 G 的极大连通子图，故 H_1 不是 G 的分图. 其中 $V_1'=\{v_1, v_2, v_3, v_4, v_6\}$，$E_1'=E_1 \cup \{v_3, v_4\}$.

H_2 是 G 的子图，但不是连通子图，故不是 G 的分图.

H_3 是 G 的极大连通子图，因为 G 中包含 H_3 的其他任何子图都将包含 v_7, v_8, v_9 中一个结点，这样这个包含 H_3 的子图必将不连通. 所以 H_3 是 G 的分图.

例 8-11 已知关于人员 a，b，c，d，e，f 和 g 的下述事实：

a 说英语；

b 说英语和西班牙语；

c 说英语，意大利语和俄语；

d 说日语和西班牙语；

e 说德语和意大利语；

f 说法语，日语和俄语；

g 说法语和德语.

试问：上述 7 人中是否任意两人都能交谈（如果必要，可由其

余5人中所组成的译员链帮忙)?

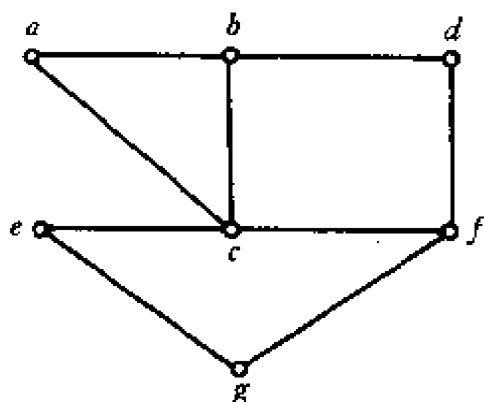


图 8-10

解 设7个人为7个结点,将两个懂同一语言的人之间连一条边.(即他们能直接交谈).这样就得到一简单图G,问题就转化为G是否连通,G如图8-10所示,因为G中任意两个结点是连接的,所以G是连通图.因此,上述7人中任意两个能交谈.

6. 有向图

一个有向图G定义为一个序偶G=(V,E),其中V是一个非空有限集合,其元素称为结点,E是V中不同元素的有序对偶的集合,其元素(v_i,v_j)称为v_i到v_j的边,v_i为边的始点,v_j为终点.

有向图与无向图的区别在于边集E是"有序对偶"的集合,即$v_i \neq v_j$时,$(v_i,v_j)\neq(v_j,v_i)$.若存在一条从结点v_i到v_j的有向路,则称从v_i到v_j是可达的.

例8-12 设G=(V,E)是一有向图,如图8-11所示,

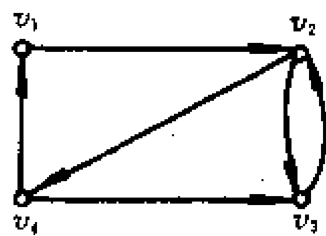


图 8-11

(1)在G中找一条长为4的有向开路且不是真路;

(2)在G中找一条长为3的有向真路;

(3)在G中找一个长为6的有向回路且不是环路;

(4)在G中找一个长为3的有向环路;

(5)求$d(v_1,v_3)$和$d(v_3,v_1)$

解 (1)l_1:$v_1v_2v_4v_3v_2$(因为v_2出现二次,所以不是有向环路);

(2)l_2:$v_1v_2v_4v_3$;

(3)l_3：$v_1v_2v_4v_3v_2v_4v_1$(因为 v_2，v_4 均重复出现，所以不是有向环路)；

(4)l_4：$v_1v_2v_4v_1$；

(5)$d(v_1,v_3)=2$，$d(v_3,v_1)=3$；

例 8-13 判定图 8-12 给出的两图分别是否为弱连通的，单向连通的，强连通的.

解 (1)将 G_1 与 G_2 中边的方向略去后，显然得到两个连通的无向图，故 G_1 与 G_2 均是弱连通的.

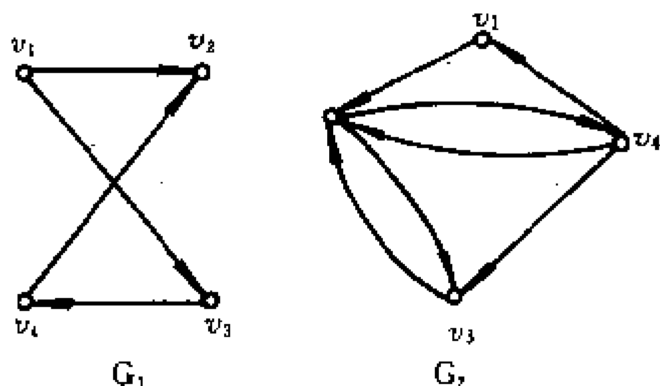


图 8-12

(2)在 G_1 中 v_1 到 v_4 有一条有向路 $v_1v_3v_4$，故 v_1 可达 v_4，类似可知，v_1 可达 v_2，v_1 可达 v_3，v_3 可达 v_2，v_4 可达 v_2，v_3 可达 v_4，即 G_1 中任意两结点中至少有一个由另一个可达，即单向可达，所以，G_1 是单向连通的，类似可判定 G_2 也是单向连通的.

(3)在 G_1 中 v_1 可达 v_4，但 v_4 不可达 v_1，故 v_1 与 v_4 不是相互可达的，所以 G_1 不是强连通的. 在 G_2 中可验证任意两结点均是相互可达的，所以 G_2 是强连通的.

7. 图的邻接矩阵和连接矩阵

给定图 $G=(V,E)$，其中 $V=\{v_1,v_2,\cdots,v_n\}$，n 阶方阵 $A=(a_{ij})$ 称为 G 的邻接矩阵，其元素 $a_{ij}=\begin{cases}1, 若\{v_i,v_j\}\in E;\\0, 否则.\end{cases}$

由邻接矩阵的积 A^l 可以得到 v_i 到 v_j 的长度为 l 的路的总数 $a_{ij}^{(l)}$，且可由 $B=A+A^2+\cdots+A^n$ 判断 G 是否为连通图. 简化运算过程得连接矩阵 $C=A[+]A^{(2)}[+]\cdots[+]A^{(n)}$ 其中[+]和[·]是布尔矩阵运算. 于是 $C=(c_{ij})$ 中的元素.

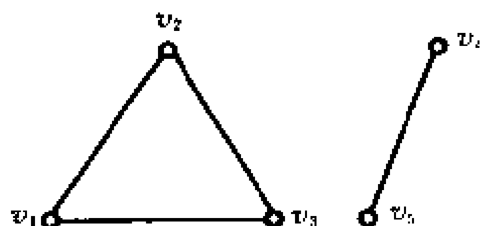


图 8-13

$$c_{ij}=\begin{cases}1, 若从 v_i 到 v_j 存在一条路；\\ 0, 否则.\end{cases}$$

例8-14 图G由邻接矩阵

$$A=\begin{bmatrix}0&1&1&0&0\\1&0&1&0&0\\1&1&0&0&0\\0&0&0&0&1\\0&0&0&1&0\end{bmatrix}$$

给出，G是否连通？

解 方法一

直接由邻接矩阵给出G的一个图解，如图8-13所示，显然，G不连通.

方法二 求G的连接矩阵

$$C = A[+]A^{(2)}[+]A^{(3)}[+]A^{(4)}[+]A^{(5)}$$

$$=\begin{bmatrix}0&1&1&0&0\\1&0&1&0&0\\1&1&0&0&0\\0&0&0&0&1\\0&0&0&1&0\end{bmatrix}[+]\begin{bmatrix}1&1&1&0&0\\1&1&0&0&0\\1&1&1&0&0\\0&0&0&1&0\\0&0&0&0&1\end{bmatrix}$$

$$[+]\begin{bmatrix}1&1&1&0&0\\1&1&1&0&0\\1&1&1&0&0\\0&0&0&0&1\\0&0&0&1&0\end{bmatrix}[+]\begin{bmatrix}1&1&1&0&0\\1&1&1&0&0\\1&1&1&0&0\\0&0&0&1&0\\0&0&0&0&1\end{bmatrix}$$

$$[+]\begin{bmatrix}1&1&1&0&0\\1&1&1&0&0\\1&1&1&0&0\\0&0&0&0&1\\0&0&0&1&0\end{bmatrix}=\begin{bmatrix}1&1&1&0&0\\1&1&1&0&0\\1&1&1&0&0\\0&0&0&1&1\\0&0&0&1&1\end{bmatrix}.$$

因为C中含有0元素，所以G不连通.

8. 割边和割点

给定图 G＝(V,E)，若在 G 中删去边 $e=\{v_i,v_j\}$ 后，得到图 G－e，其分图数比 G 的分图数增加，则称 e 是 G 的割边．若在 G 中删去结点 v 及与其相关联的所有边后，得到图 G-v，其分图数比 G 的分图数增加，则称结点 v 是 G 的割点．

e 是图 G 的割边的充要条件是，e 不在 G 的任何环路中出现．

v 是图 G 的割点的充要条件是，存在两个结点 u 和 w($u\neq v\neq w$)，使得连接 u 和 w 的所有路中都出现结点 v．

例 8-15 给定图 G 如图 8-14 所示，求 G 的割边和割点．

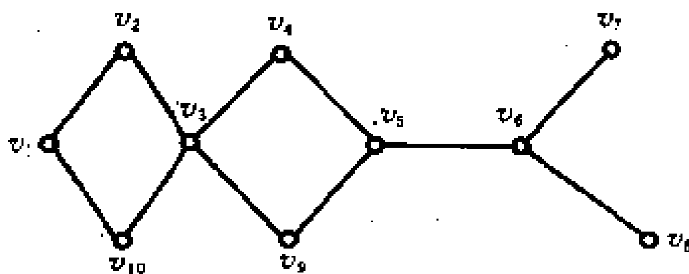


图 8-14

解 $e_1=\{v_6,v_5\}$，$e_2=\{v_6,v_7\}$，$e_3=\{v_6,v_8\}$均是 G 的割边，v_3，v_5，v_6 均是 G 的割点．

例 8-16 一个 n 阶连通图 G 最少有几个割点？最多有几个割点？

解 当 G 是一个 n 阶完全图时，从 G 中去掉任意结点都不增加 G 的分图数，此时 G 的割点数为 0．

一个 n 阶连通图 G，当他无环路且为一条真路时，割点数最多．此时 G 的割点数为 $n-2$．

9. 图的连通性

设图 G＝(V,E)是一连通图，若 $S\subseteq E$ 使得在图 G 中删去了

S 中的所有边后，得到的子图 $G-S$ 变成具有两个分图的不连通图，而删去了 S 的任一真子集后，得到的子图仍是连通图，则称 S 是 G 的一个边割集.

设图 $G=(V,E)$ 是一连通图，$V_1\subseteq V$，G 中端点分别属于 V_1 和 $V_1'(=V-V_1)$ 的所有边的集合，称为 G 的断集.

边割集是断集的一个特例.

设图 $G=(V,E)$ 是一连通图，若有 V 的子集 V_1 使得在图 G 中删除了 V_1 中的所有结点后，所得到的子图 $G-V_1$ 不连通或为平凡图(即(1,0)图)，则称 V_1 是 G 的一个点割集.

割点是点割集的一个特例.

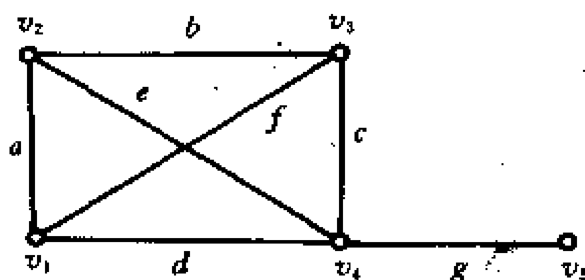


图 8-15

例 8-17 求图 8-15 中的几个边割集，断集和点割集.

解 $S_1=\{a,f,d\}$，$S_2=\{a,e,b\}$，$S_3=\{b,c,f\}$，$S_4=\{c,f,d\}$，$S_5=\{g\}$，$S_6=\{a,e,f,c\}$，$S_7=\{b,d,e,f\}$均是 G 中的边割集.

取 $V_1=\{v_2,v_3,v_5\}$则 $V_1'=\{v_1,v_4\}$.

$S'=\{a,e,f,c,g\}$是 G 的一个断集，且 $S'=S_6\cup S_5$，

取 $V_2=\{v_3,v_4,v_5\}$，则 $V_2'=\{v_1,v_2\}$.

$S_2'=\{b,d,e,f\}$是 G 的一个断集. 且 $S_2'=S_7$

$V_3=\{v_4\}$是 G 的点割集，且 v_4 是割点.

$V_4=\{v_1,v_4\}$，$V_5=\{v_3,v_4\}$，$V_6=\{v_2,v_4\}$均是 G 的点割集.

10. 点的连通度和边的连通度

G 的点的连通度：设 $G=(V,E)$ 是连通图，则 $K(G)=\min\{\#V_i|V_i$ 是 G 的点割集$\}$称为 G 的点连通度(或连通度).

G 的边连通度：设 $G=(V,E)$ 是连通图，则 $\lambda(G)=\min\{\#S|S$ 是 G 的断集$\}$称为 G 的边连通度.

定理 8.10.1 对任意的图 $G=(V,E)$，有 $K(G)\leqslant\lambda(G)\leqslant\delta(G)$. 其中 $K(G)$，$\lambda(G)$，$\delta(G)$ 分别为 G 的点连通度，边连通度，最小度.

例 8-18 图 8-16 给出了连通图 G，求 G 的连通度 $K(G)$，边连通度 $\lambda(G)$ 和最小度 $\delta(G)$.

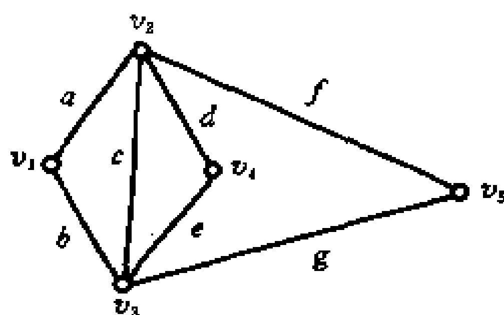


图 8-16

解 由定义知 $\delta(G)=2$

$\because S=\{f,g\}$ 是 G 中的一边割集且是 G 中含边数最少的断集.

$\therefore \lambda(G)=2$.

又 $\because V_1=\{v_2,v_3\}$ 是 G 的基数最小的点割集.

$\therefore K(G)=2$.

例 8-19 若 G 是 n 阶简单图($n>3$)，且 $\delta(G)\geqslant n-2$，则 $K(G)=\delta(G)$.

证 因为 $\delta(G)\geqslant n-2$，且 G 是 n 阶简单图所以 $\delta(G)\leqslant n-1$.

(1)若 $\delta(G)=n-1$，则 G 是 n 阶完全图，于是

$$\lambda(G)=K(G)=n-1.$$

(2)若 $n-2\leqslant\delta(G)<n-1$，即 $\delta(G)=n-2$，则 G 中存在结点 u，满足 $\deg(u)=n-2$.

从而 u 与 G 中另一结点 v 不邻接，并且 $\deg(v)=n-2$，但对于 $\forall\ w\in V, w\neq u, w\neq v$，有 $\{w,u\}\in E$，$\{w,v\}\in E$.

因此，对于 V 中任意 $n-3$ 个结点的集合 V_1，$G-V_1$ 一定是连通的，所以

$$K(G)\geqslant n-2.$$

又由定理知 $K(G)\leqslant\delta(G)$，故 $K(G)=\delta(G)$.

11. 欧拉图

在图 G 中，通过 G 的每条边一次且仅一次的回路称为欧拉回路. 具有欧拉回路的图称作欧拉图(Euler). 通过 G 的每条边一次

且仅一次的开路称为图 G 的欧拉路.

需要提醒注意的是,欧拉回路要求边不重复,但结点可重复,故欧拉回路不一定是环路.

定理 8.11.1(欧拉定理) 一个连通图 G 为欧拉图的充要条件是 G 的每一结点的度数为偶数.

定理 8.11.2 连通图 G 具有一条连接 u 到 v 的欧拉路的充要条件是,u 和 v 是 G 中仅有的奇度数结点.

例 8-20 图 8-17 给出了图 G_1,G_2,试判定哪个是欧拉图,哪个图有欧拉路,并找出一条欧拉路或欧拉回路.

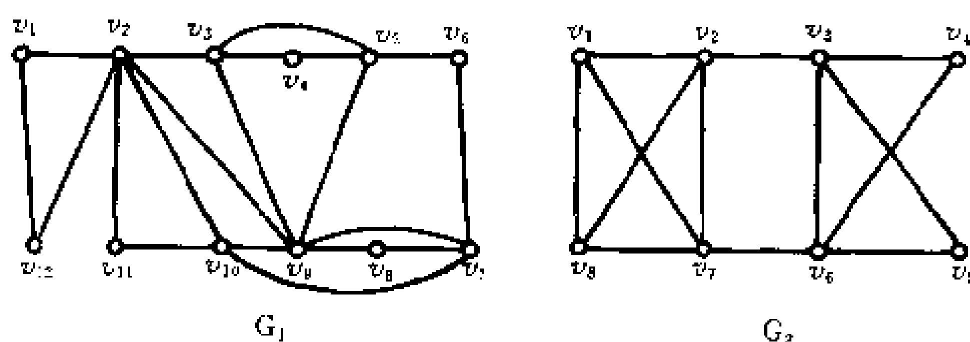


图 8-17

解 (1)因 G_1 中每个结点的度数为偶数,故 G_1 是欧拉图

$$\alpha = v_1v_2v_3v_4v_5v_6v_7v_8v_9v_5v_3v_9v_7v_{10}v_{11}v_2v_{10}v_9v_2v_{12}v_1$$

(2)因为 G_2 中 $\deg(v_1)=\deg(v_8)=3$,且其它结点度数均为偶数.

所以 G_2 有欧拉路

$$\beta = v_1v_2v_3v_4v_6v_5v_3v_6v_7v_2v_8v_7v_1v_8.$$

例 8-21 确定 n 取怎样的值,n 阶完全图 K_n 为欧拉图.

解 n 阶完全图 K_n 有 n 个结点,每个结点的度数为 $n-1$,故当 n 为奇数,$n-1$ 为偶数时,K_n 是一欧拉图.

例 8-22 若图 G 为欧拉图,则 G 中没有割边.

证 用反证法. 设 $e=\{u,v\}$是 G 的一割边,因为 G 是欧拉图,

所以 e 必在 G 的一个欧拉回路 α 上. 故从 α 中删去边 e 得连接 u 与 v 的一条路 β，由定理 8.5.1 知可得一条连接 u 与 v 的真路 L，于是 e 在 $L\cup\{e\}$ 的环路中，e 不是割边. 矛盾.

因此，假设错误，G 中没有割边.

12. 哈密顿图

通过图 G 的每个结点一次且仅一次的环路称为哈米顿环. 具有哈米顿环的图称为哈米顿图. 通过图 G 的每个结点一次且仅一次的开路称为哈米顿路.

例 8-23 图 8-18 给出了三个图，试判定哪个是欧拉图，哪个是哈密顿图，哪个图有欧拉路.

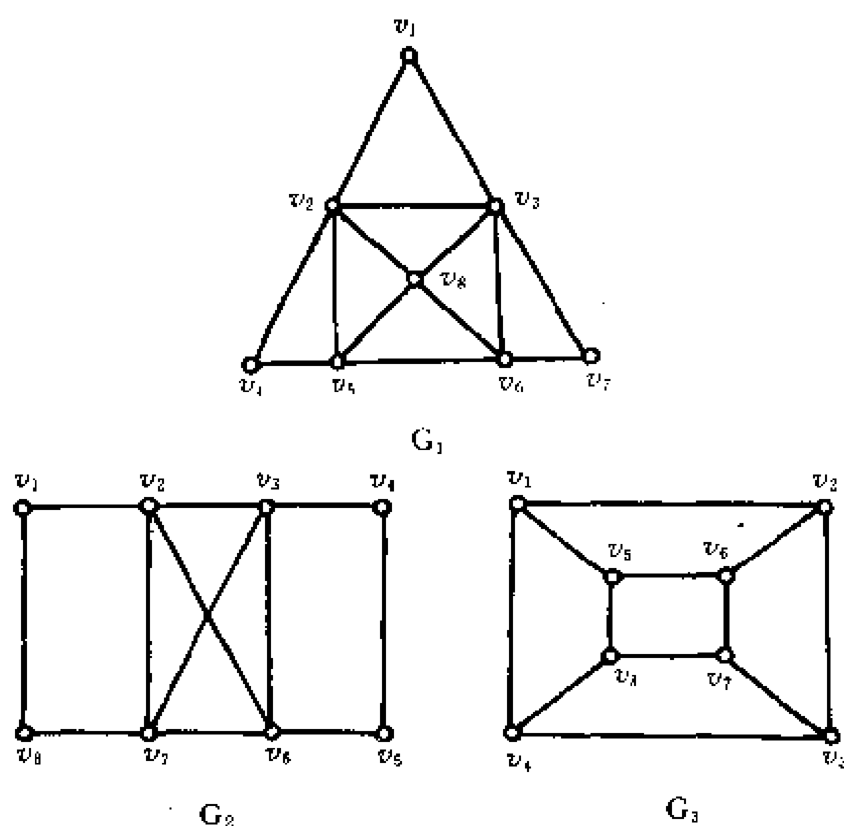


图 8-18

解　(1)G_1 中除 v_2, v_3 度数为奇数外，其余结点均是偶数. 故 G_1 中有欧拉路 $v_2v_1v_3v_2v_4v_5v_8v_2v_5v_6v_8v_3v_6v_7v_3$，又 $v_1v_3v_7v_6v_8v_5v_4v_2v_1$ 是 G_1 的哈密顿环，所以 G_1 是哈密顿图.

(2)G_2 中每个结点的度数为偶数，故 G_2 是欧拉图，其一个欧拉回路为 $v_1v_2v_7v_3v_2v_6v_3v_4v_5v_6v_7v_8v_1$ 且 $v_1v_2v_3v_4v_5v_6v_7v_8v_1$ 是 G_2 的一个哈密顿环，所以 G_2 也是哈密顿图.

(3)因为 G_3 中每个结点的度数均是奇数，所以 G_3 既不是欧拉图，也没有欧拉路，但 G_3 中有 $v_1v_2v_3v_4v_8v_7v_6v_5v_1$ 哈密顿环，因此，G_3 是哈密顿图.

13. 哈密顿图的判定问题

哈密顿环的存在性问题至今未解决，因此只能给出一个连通图是哈密顿图的几个必要条件或充分条件.

定理 8.13.1　若图 $G=(V,E)$ 是哈密顿图，则对于 V 的任何一个非空子集 S，有 $W(G-S) \leqslant \#S$，其中 $W(G-S)$ 表示 $G-S$ 中分图的个数.

注　该定理是判定一个图是否为哈密顿图的必要条件，因此，可用它说明某些图不是哈密顿图，但满足此条件的图不一定是哈密顿图.

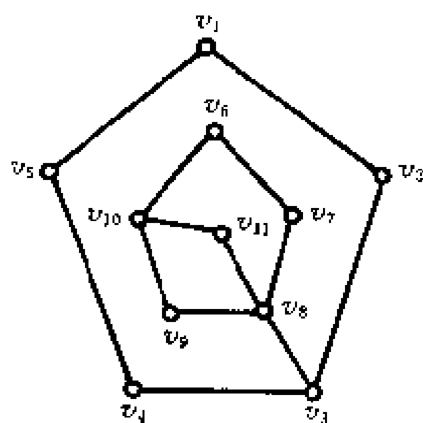


图 8-19

例 8-24　判断图 8-19 是否为哈密顿图

解　取 $S=\{v_8\}$，则 $\#S=1$，有

$$W(G-S)=2>\#S$$

因此，G 不是哈密顿图.

闭图　设 $G=(V,E)$ 是 n 阶图，若对 $\deg(u)+\deg(v) \geqslant n$ 的每一对结点 u 和 v，均有 $\{u,v\} \in E$（即

u 与 v 邻接)，则称图 G 是闭图.

闭包 图 G 的闭包 G_c 是一个与 G 有相同的结点集的闭图，且 G_c 是包含 G 的最小的闭图(即 $G \subseteq G_c$，若 $G \subseteq H \subseteq G_c$ 且 $H \neq G_c$，则 H 不是闭图).

给定图 G，可构造出它的闭包 G_c，其步骤如下：

(1)令 $G=G_1$，$1 \to i$

(2)若 G_i 是一个闭图，则 $G_c=G_i$；否则

(3)在 G_i 中找出满足以下两个条件的结点 u 和 v：

　　i)$\deg(u)+\deg(v) \geqslant n$；

　　ii)u 和 v 不相邻接.

将边 $\{u,v\}$ 加到图 G_i 中，得 $G_{i+1}=G_i+\{u,v\}$

(4)$i+1 \to i$，并返回到第(2)步.

定理 8.13.2 设有图 $G=(V,E)$，当且仅当 G_c 是哈密顿图时，图 G 是哈密顿图.

推论 1 若图 G 的闭包 $G_c=K_n$，且 $n \geqslant 3$，则 G 是哈密顿图.

推论 2 设图 $G=(V,E)$，$\#V=n$，$n \geqslant 3$，若对于任意的 $v \in V$，均有 $\deg(v) \geqslant \frac{n}{2}$，则 G 是哈密顿图.

推论 3 设图 $G=(V,E)$，$\#V=n$，$n \geqslant 3$，若 V 中任意两个不相邻的结点 u 和 v，均有 $\deg(u)+\deg(v) \geqslant n$，则 G 是哈密顿图.

例 8-25 构造图 8-20 中图 G 的闭包，并判别图 G 是否为哈密顿图？如图不用观察的方法，你能说出你判别的根据吗？**解** 先求图 G 的闭包 $n=6$ 因为

$$\deg(v_5)+\deg(v_6)=6;$$

$$\deg(v_2)+\deg(v_3)=6,$$

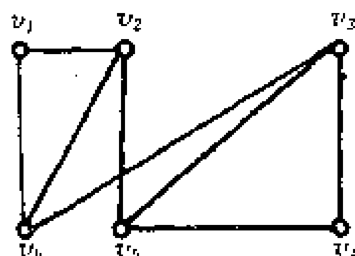


图 8-20

所以连接 v_5 与 v_6，v_2 与 v_3 得图 G_2. 在图 G_2 中，因

$$\deg(v_2)+\deg(v_4)=6;$$

$$\deg(v_1) + \deg(v_5) = 6;$$
$$\deg(v_4) + \deg(v_6) = 6;$$
$$\deg(v_1) + \deg(v_3) = 6,$$

故连接 v_2 与 v_4，v_1 与 v_5，v_4 与 v_6，v_1 与 v_3 得图 G_3. 在图 G_3 中，因

$$\deg(v_1) + \deg(v_4) = 8$$

故连接 v_1 与 v_4 得 G_4，且 G_4 是 G 的闭包，即 $G_c = G_4 = K_6$ 如图 8-21 所示.

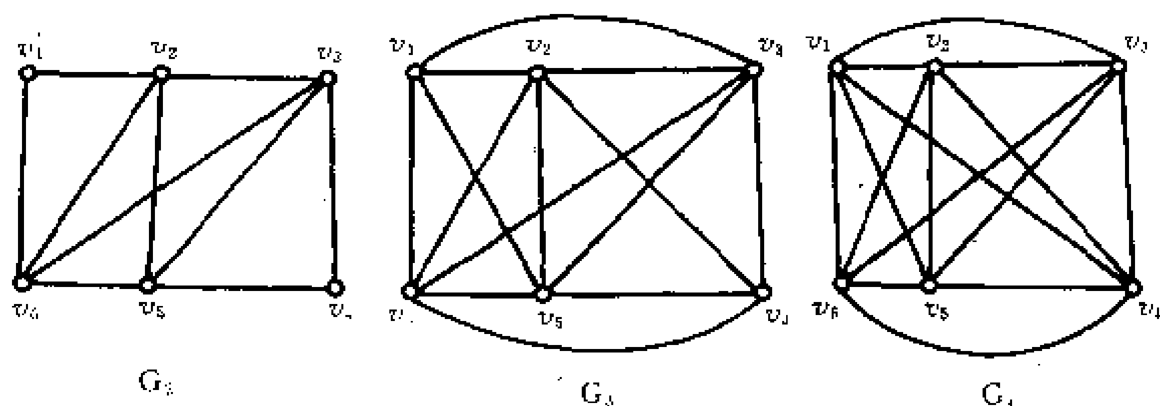


图 8-21

由定理 8.13.2 的推论 1 知 G 是哈密顿图.

14. 树及树林

不含环路的连通图称为树. 不含环路的图称为树林（或森林）. 树中度为 1 的结点称为树叶，度数大于 1 的结点称为分枝结点.

树的特征可以从多方面来刻画，下述定理给出了判断一个 (n, m) 图 T 为树的三个必要充分条件，这些条件中的每一个都是树所具有的特性，且均可作为树的一种定义.

定理 8.14.1 设 (n,m) 图 T 是树的必要充分条件：

(1) T 是 $m=n-1$ 的连通图.

(2) T 是 $m=n-1$ 且无环路的图.

(3) T 是每两个结点之间由唯一的真路相连接的图.

定理 8.14.2 设 T 是结点数为 $n(n\geqslant 2)$ 的无向树，则 T 中至少有两片树叶.

例 8-26 判定下面各类图是否为树.

(1)有 n 个结点，$n-1$ 条边的连通图；

(2)每对结点间都有路的图；

(3)有 n 个结点，$n-1$ 条边的图.

解 (1)由定理 8.14.1(1)知此类图为树.

(2)该类图不一定是树，其条件只能保证图是连通图. 如图 8-22 中 G_1 满足条件，但不是树.

(3)该类图不一定是树，条件只能保证 $m=n-1$，如图 8-22 中，G_2 满足条件，但不是树，因为 G_2 不连通.

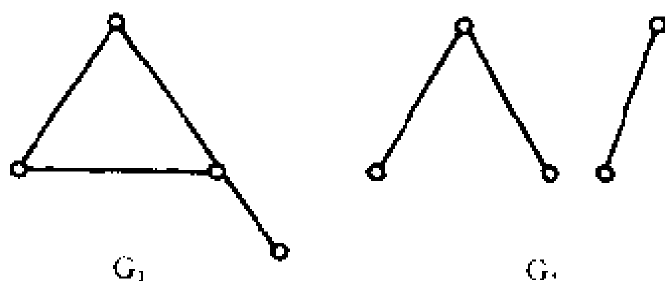


图 8-22

例 8-27 设 G 是简单连通图，G 是树，当且仅当 G 的每条边为割边.

证 必要性 假设 G 是一棵树，$G=(V,E)$，由于 G 不含环路，所以 G 的每条边 e 均不在 G 的任何环路上，故 e 是割边.

充分性 若 G 连通，但不是树，则 G 中有环路 C，设 e 是 C 上的任意一条边，则 e 不是割边，与条件矛盾. 所以 G 是树.

例 8-28 一棵树 T 有两个结点度数为 2，一个结点度数为 3，三个结点度数为 4，问它有几个叶结点.

解 设 T 有 n 个结点，m 条边，x 个叶结点，则 $n=2+1+3+x=6+x$.

由定理 8.14.1 知 $m=n-1=5+x$，又由握手定理知

$2m=2\times2+3\times1+4\times3+1\times x=19+x$

故 $2\times(5+x)=19+x \qquad x=9$

因此,T 有 9 个叶结点.

15. 生成树

如果 T 是图 $G=(V,E)$ 的一个生成子图,且是一棵树,则称 T 是图 G 的一棵生成树. G 中属于 T 的边称为 T 的枝,G 中属于 E,不属于 T 的边称为 T 的弦.

每个连通图 G,一定有生成树. 如何求 G 的生成树呢?

破坏法:若 G 中无环路,则 G 就是最小生成树. 若 G 中有环路,则任取一个环 σ,删除 σ 上任一边,继续这一过程,直到图中无环为止,所得图即为 G 中一棵生成树.

例 8-29 图 8-23 给出了一个连通图 G,求 G 的一棵生成树 T_G,并指出 T_G 的二条枝和二条弦.

解 $G_1=G$ 中有环 $\sigma_1=v_1v_2v_5v_7v_1$ 删去边 $\{v_1,v_2\}$ 得 $G_2=G_1-\{v_1,v_2\}$,见图 8-24.

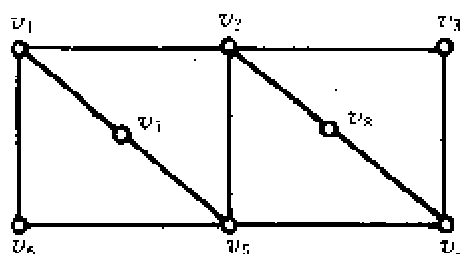


图 8-23

G_2 中有环 $\sigma_2=v_2v_3v_4v_8v_2$,删去边 $\{v_2,v_3\}$ 得 $G_3=G_2-\{v_2,v_3\}$;

G_3 中有环 $\sigma_3=v_1v_7v_5v_6v_1$,删去边 $\{v_1,v_6\}$ 得 $G_4=G_3-\{v_1,v_6\}$;

G_4 中有环 $\sigma_4=v_2v_8v_4v_5v_2$,删去边 $\{v_4,v_5\}$ 得 $G_5=G_4-\{v_4,v_5\}$,

G_5 无环,故 $T_G=G_5$ 是 G 的一棵生成树. $\{v_1,v_7\}$ $\{v_6,v_5\}$ 是 T_G 的二条枝,$\{v_1,v_2\}$,$\{v_2,v_3\}$ 是 T_G 的二条弦.

16. 最小生成树

设 $G=(V,E,f)$ 是一连通的有权图,其中 f 是 E 到 R 的函数,若 T 是 G 的一棵生成树,F 的树枝的集合为 $E(T)$,则 T 中所

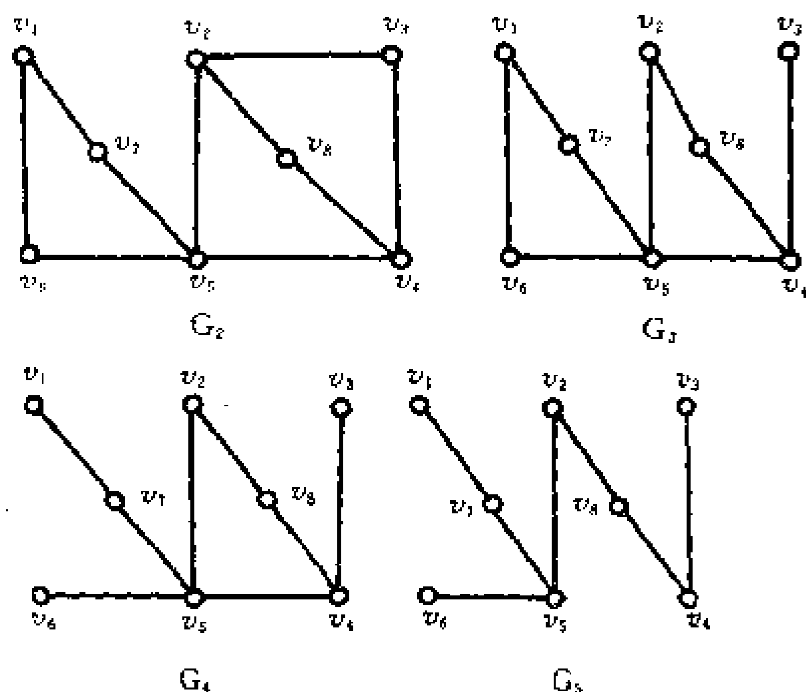


图 8-24

有树枝的权的和 $W(T)=\sum_{e\in E(T)}f(e)$ 称为 T 的权，G 中具有最小权的生成树 T，称为 G 的最小生成树.

避环法：设 $G=(V,E,f)$ 是一具有 n 个结点的连通有权图，G 的边按权的递增顺序排列为 $f(a_1)\leqslant f(a_2)\leqslant\cdots\leqslant f(a_m)$，取 $e_1=a_1$，$e_2=a_2$ 在 T 中；检查 a_3，若 a_3 不与已在 T 中的边构成环，则取 $e_3=a_3$ 在 T 中，否则放弃 a_3，再检查 a_4，继续这一过程，直到形成生成树 T 为止，所得 T 为最小生成树.

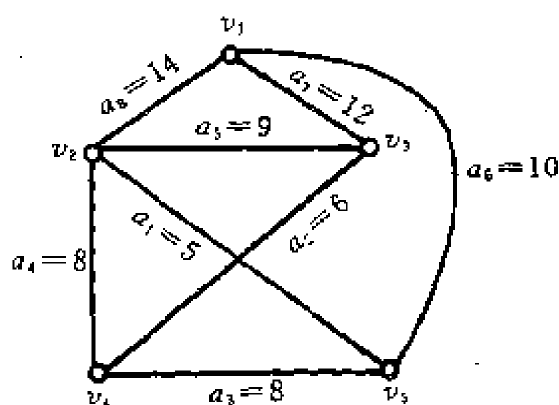


图 8-25

例 8-30 在图 8-25 所示的有权图 G 中，求一棵最小生成树 T，并计算其权.

解 $f(a_1)=5$ $f(a_2)=6$

$f(a_3)=8$　$f(a_4)=8$　$f(a_5)=9$　$f(a_6)=10$　$f(a_7)=12$　$f(a_8)=14$ 取 $e_1=a_1=\{v_2,v_5\}$，$e_2=a_2=\{v_3,v_4\}$ 由于 $\{v_4,v_5\}=a_3$ 与 e_1，e_2 不构成环路，所以取 $e_3=\{v_4,v_5\}$，而 $a_4=\{v_2,v_4\}$ 和 $a_5=\{v_2,v_3\}$ 均与 $\{e_1,e_2,e_3\}$ 构成环路，故选 $e_4=a_6=\{v_1,v_5\}$ 即 $T=\{e_1,e_2,e_3,e_4\}$ 如图 8-26 所示

$$W(T)=5+6+8+10=29.$$

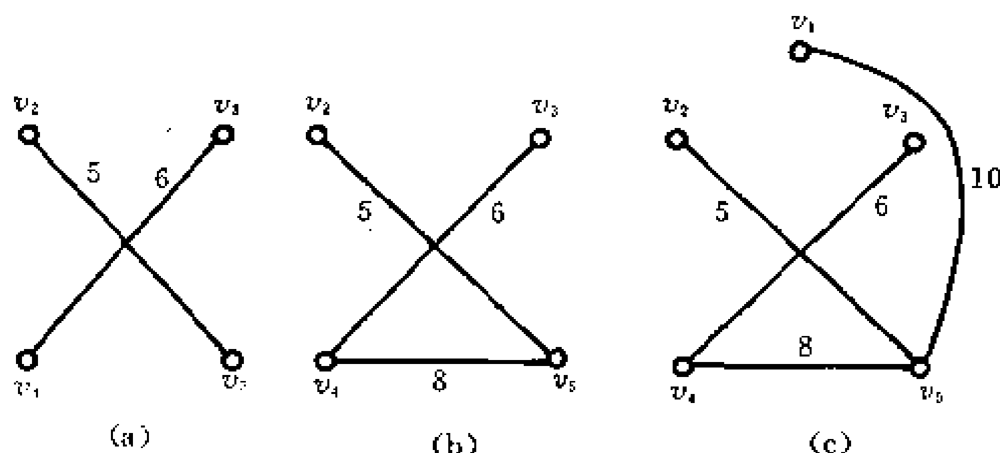


图 8-26

17. 有向树

一个不包含环的有向图 G，若它只有一个结点 v_0 的入度是 0，而所有其他结点的入度都等于 1，则称 G 为有向树，v_0 为树根，出度为 0 的结点称为树叶，不是树叶的其他结点称为分枝结点.

设 T 为一棵有向树，若 T 中每个结点的出度至多为 m，则称 T 为 m 元树，若 T 中每个结点的出度为 0 或 m，则称 T 为完全 m 元树.

定理 8.17.1　设 T 是一棵 (n,m) 有向树，则 $m=n-1$.

例 8-31　试证完全二元树有奇数个结点.

证　设 T 是一棵完全二元树，T 为 (n,m) 图，T 有 n_0 片树叶，则 T 有 $n-n_0$ 个分枝结点. 于是 $m=2(n-n_0)$，又 $m=n-1$，所以 $n-1=2n-2n_0$。因此，$n=2n_0-1$，为奇数.

例 8-32 将图 8-27 给出的三元树转化为二元树.

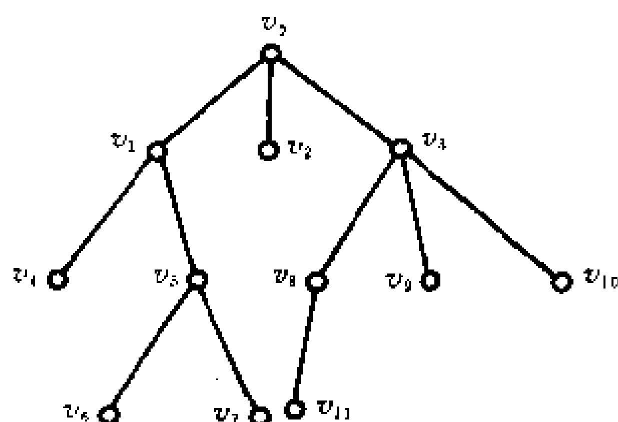


图 8-27

解 (1)对每一结点只保留它的最左分枝,删去其余分枝;

(2)在同一级上的结点从左到右用边连接起来;

(3)对任一结点选定在该结点下的结点为它的左儿子,在该结点右边的为它的右儿子.

(4)将结点的左儿子画在结点的左下方,右儿子画在结点的右下方,如图 8-28(3)所示.

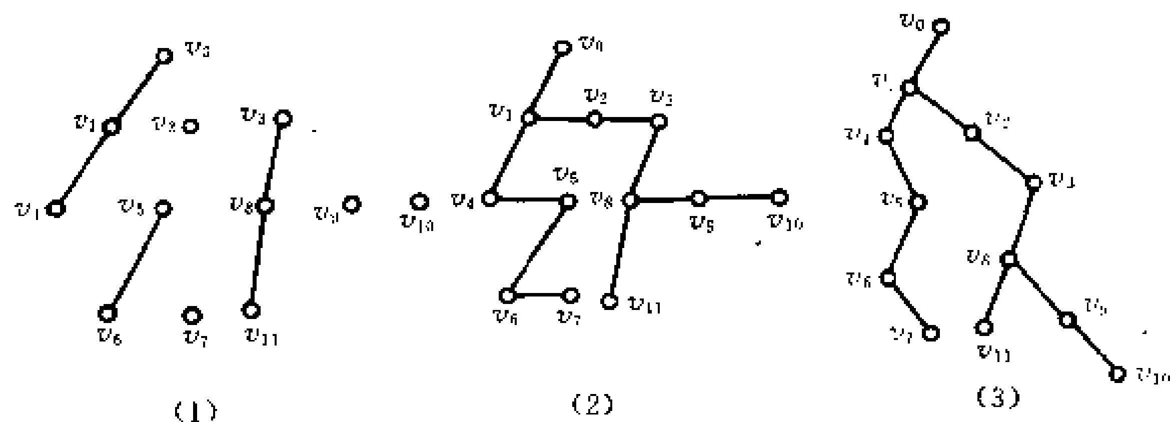


图 8-28

例 8-33 分别用先根通过,中根通过和后根通过的算法扫描图 8-28(3)所示的二元树 T 的所有结点.

解 (1)先根通过

先访问根结点,然后在根结点的左子树上执行先根通过算法(即在以根结点的左儿子为根的子树上执行该算法),最后在根结点的右子树上执行先根通过算法.

先根通过 T 扫描结果为 $v_0v_1v_4v_5v_6v_7v_2v_3v_8v_{11}v_9v_{10}$

(2)中根通过

先在根结点的左子树上执行中根通过算法,然后访问根结点;最后在根结点的右子树上执行中根通过算法.

在 v_0 的左子树上执行中根通过,v_0 的左子树以 v_1 为根,由于 v_1 有左子树,以 v_4 为根,所以再在以 v_4 为根的子树上执行中根通过. 因为 v_4 无左子树,故扫描 v_4,然后再在 v_4 的右子树,即以 v_5 为根的子树上执行中根通过,继续这一过程……,最后扫描结果为 $v_4v_6v_7v_5v_1v_2v_{11}v_8v_9v_{10}v_3v_0$.

(3)后根通过

先在根的左子树上执行后根通过算法;然后在根的右子树上执行后根通过算法;最后访问根结点扫描结果为 $v_7v_6v_5v_4v_{11}v_{10}v_9v_8v_3v_2v_1v_0$

18. 二部图

二部图:若图 $G=(V,E)$ 的结点集 V 能分成两个互不相交的子集 V_1 和 V_2(即 $V=V_1\cup V_2, V_1\cap V_2=\varnothing$),使得 G 中每条边的端点,一个属于 V_1,另一个属于 V_2,则称 G 为二部图(或称为二分图). 记 $G=(V_1,V_2,E)$.

由二部图的定义知:V_1(或 V_2)中任意两个结点不邻接.

完全二部图:设 $G=(V_1,V_2,E)$ 是一个二部图,若 V_1 中每个结点与 V_2 的每个结点邻接,则称 G 为完全二部图,记作 $K_{m,n}$,其中 $\#V_1=m$, $\#V_2=n$.

定理 8.18.1 图 G 为二部图的充要条件是它的所有回路均为偶数长.

例 8-34 完全二部图 $K_{m,n}=(V_1,V_2,E)$ 中共有多少条边?

解 因为 V_1 中每个结点都与 V_2 中每个结点相邻接,所以 V_1 中每个结点关联 $\#V_2=n$ 条边,而 V_1 中有 m 个结点,因此,$K_{m,n}$ 共有 m,n 条边.

例 8-35 图 8-29 是否为二部图？若是，找出它的互补结点集.

解 是二部图. 其中 $V_1=\{v_1,v_3,v_5,v_7\}$
$V_2=\{v_2,v_4,v_6\}$.

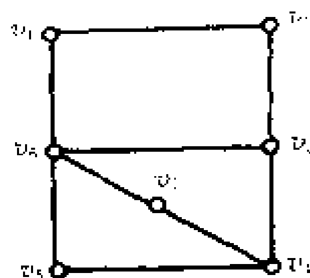


图 8-29

19. 匹配

设 $G=(V_1,V_2,E)$ 是二部图，其中 $V_1=\{v_1,v_2,\cdots,v_q\}$，对 V_1 中每一结点 v_i 都取一条边 $\{v_i,v_i'\}\in E$，这些无公共结点的 q 条边组成一个 V_1 对 V_2 的匹配.

V_1 对 V_2 存在匹配的必要条件是 $\# V_1\leqslant \# V_2$.

定理 8.19.1 设 $G=(V_1,V_2,E)$ 是一个二部图，则 G 中存在 V_1 对 V_2 的匹配的充要条件是：V_1 中每 k 个结点（$k=1,2,\cdots,\# V_1$）至少和 V_2 中 k 个结点相连接. 该条件称为相异性条件.

定理 8.19.2 设 $G=(V_1,V_2,E)$ 是一个二部图，则 G 中存在 V_1 对 V_2 匹配的充分条件是：存在某一整数 $t>0$，使得

(1)V_1 中的每个结点，至少有 t 条边与其相关联；

(2)V_2 中的每个结点，至多有 t 条边与其相关联.

((1)，(2)统称为 t-条件).

例 8-36 判定图 8-30 所给出的三个二部图是否存在 V_1 对 V_2 的匹配？

解 (1)G_1 满足 $t=2$ 时的 t-条件，即 V_1 中每个结点至少与 2 条边相关联，V_2 中每个结点至多与 2 条边相关联，所以，G_1 中存在 V_1 对 V_2 的匹配. 如图 8-31 所示.

(2)图 G_2 不满足相异性条件，如 $k=2$ 时，V_1 中两结点 v_2,v_3 只与 V_2 中一个结点 v_6 相连接，故 G_2 中不存在 V_1 对 V_2 的匹配.

(3)在 G_3 中，因为 V_1 中结点至少关联二条边，应有 $t=2$，而 V_2 中结点至多与 3 个结点相关联. 所以不满足 t 条件，尽管如此，但 V_1 中任意 $k(=1,2,3)$ 个结点至少与 V_2 中 k 个结点相连接，即满足相异性条件，所以 G_3 中存在 V_1 对 V_2 的匹配. 如图 8-32.

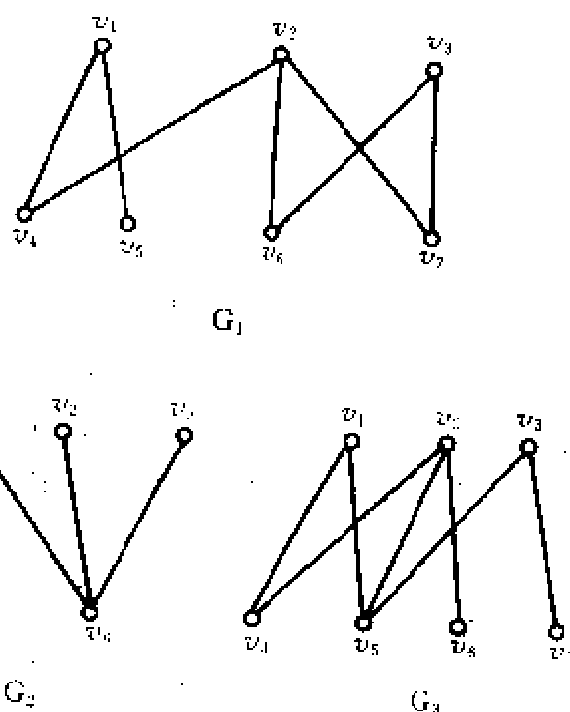


图 8-30

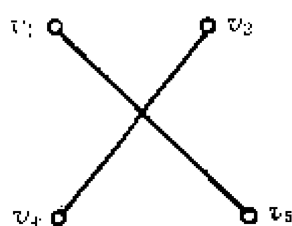


图 8-31

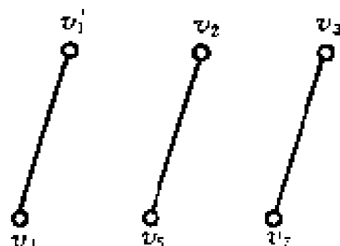


图 8-32

例 8-37 现有 3 个课外小组：物理组，化学组和生物组．今有张、王、李、赵、陈 5 名同学．已知：

(1)张，王为物理组成员，张、李、赵为化学组成员，李、赵、陈为生物组成员．

(2)张为物理组和化学组成员，王、李、赵、陈为生物组成员．

问在(1)，(2)二种情况下能否各选出 3 名不兼职的组长？为什么？

解　可以将 v_1,v_2,v_3 分别看作是物理，化学和生物三个课外小组，v_4,v_5,v_6,v_7,v_8 分别看作张、王、李、赵、陈 5 名同学，记 $V_1=\{v_1,v_2,v_3\}$，$V_2=\{v_4,v_5,v_6,v_7,v_8\}$，$V_2$ 中与 $v_i(i=1,2,3)$ 相连接的结点，可看作是该组成员，因此，问题转化为寻找一个从 V_1 到 V_2 的匹配.

(1)根据条件可做二部图，如图 8-33(1)所示. 由于 V_1 中每个结点至少与 V_2 中 2 个结点相关联，V_2 中每个结点至多与 V_1 中 2 个结点相关联，因而满足 t-条件($t=2$)，由定理 8.19.2 知存在从 V_1 到 V_2 的匹配，如图 8-33(2)所示. 因此，可以选出三名不兼职的组长张、李、赵.

(2)根据条件可做二部图如 8-33(3)所示.

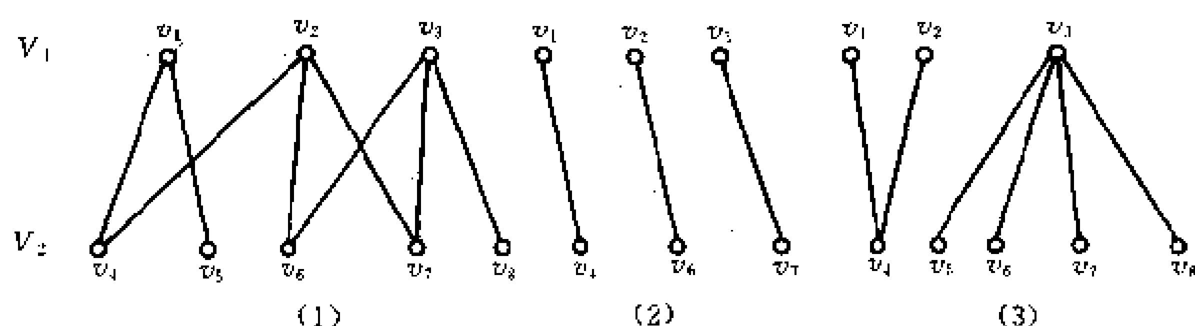


图 8-33

因为 V_1 中 v_1,v_2 两个结点只与 V_2 中一个结点相连接，不满足"相异性条件"，所以不存在 V_1 对 V_2 的匹配，故在该情况下选不出三名不兼职的组长.

20. 平面图

若一个图 G 能以一种方式画在平面上，使得除结点处之外无边相交，则称 G 为平面图，否则称图 G 为非平面图. 平面图 G 的边所包围的一个区域，其内部既不含图的结点，也不含图的边，这样的区域称为 G 的一个面，包围该面的各边所构成的回路称为该面的边界.

定理 8.20.1　设 G 是一连通的平面图，则有

$$n - m + k = 2 \qquad (*)$$

其中 n,m,k 分别是图 G 的结点数,边数和面数(包括无限面).(*)式称为关于平面图的欧拉公式.

推论 1 在有两条或更多条边的任何连通的平面图 G 中,有 $m \leqslant 3n-6$.

推论 2 在每个面至少由 4 条或更多条边围成的连通平面 G 中,有 $m \leqslant 2n-4$.

例 8-38 说明图 8-34 所示的两个图为平面图.

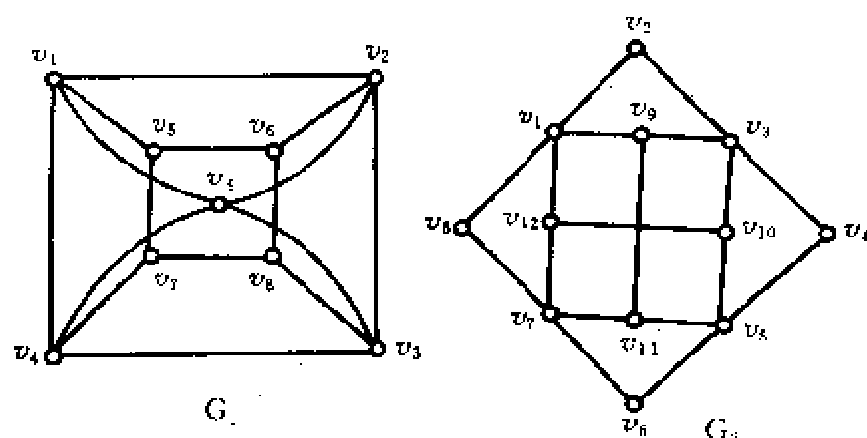


图 8-34

解 G_1,G_2 分别能画成如图 8-35(1),(2)所示的图解,故均是平面图.

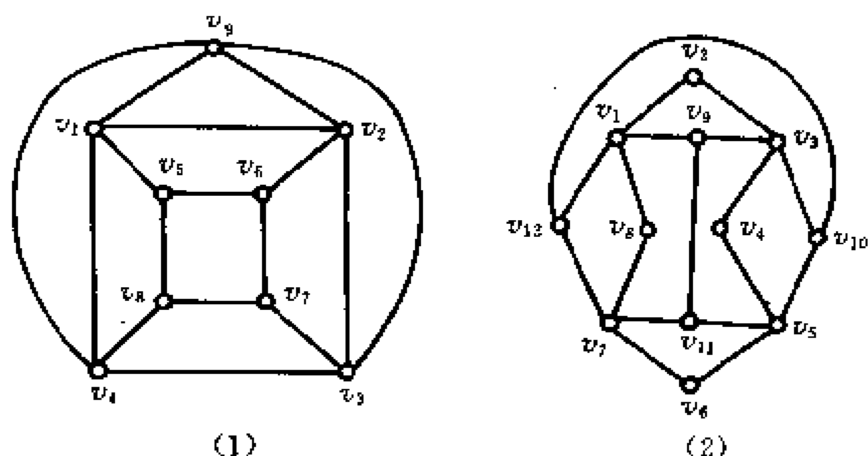


图 8-35

21. 平面图的判定

如果图 G_1 与 G_2 是同构的，或反复插入或删除度为 2 的结点后是同构的，则称 G_1 与 G_2 在度为 2 的结点内同构.

定理 8.21.1（Kuratowski 定理） 一个图是平面图的必要充分条件是，它不包含任何在度为 2 的结点内与 K_5 或 $K_{3,3}$ 同构的子图.

给定一个连通图 G，要判定它是否为平面图，首先，检测它是否满足 $m \leqslant 3n-6$，若不满足，它一定是非平面图，若满足则不能确定它是否为平面图，再利用 Kuratowski 定理检测，或尝试一下能否画一个相应的，边不相交的图解.

例 8-39 判定如图 8-36 所示的三个图是否为平面图.

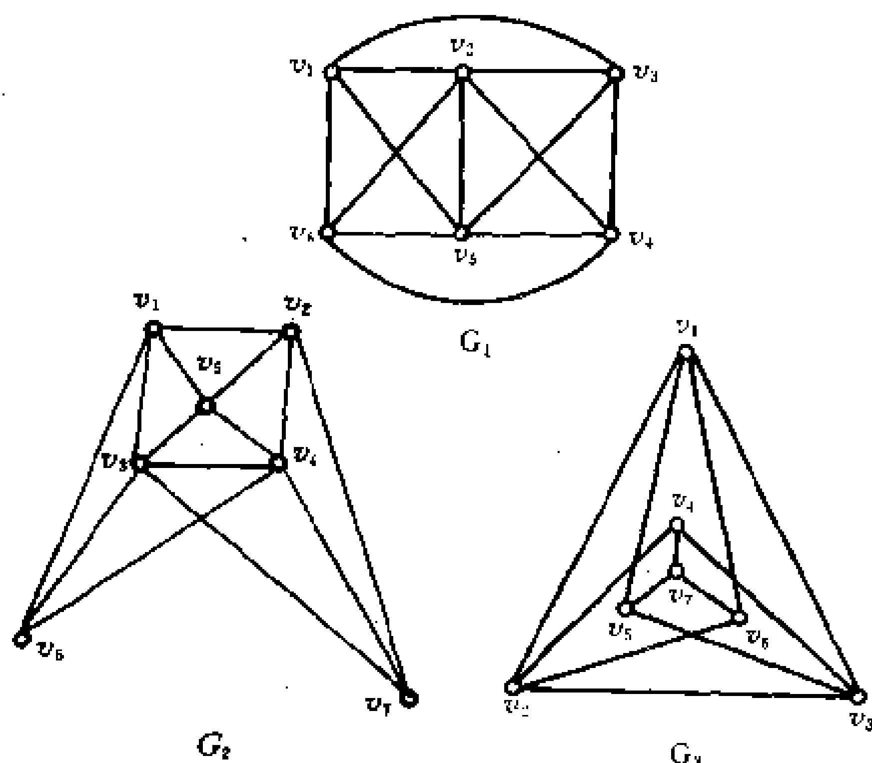


图 8-36

解 (1) G_1 的结点数 $n=6$，边数 $m=13$，G_1 连通. 若 G_1 是平面图，则 $m=13 \leqslant 3n-6=18-6=12$ 矛盾，所以 G_1 是非平面图.

(2)取 G_2 的子图 G_2' 如图 8-37(1)所示 G_2' 在度为 2 的结点内与 $K_{3,3}$ 同构，如图 8-37(2)所示，由 Kuratowski 定理知 G_2 是非平面图.

(3)G_3 能画出如图 8-37(3)所示的平面图解，故是平面图.

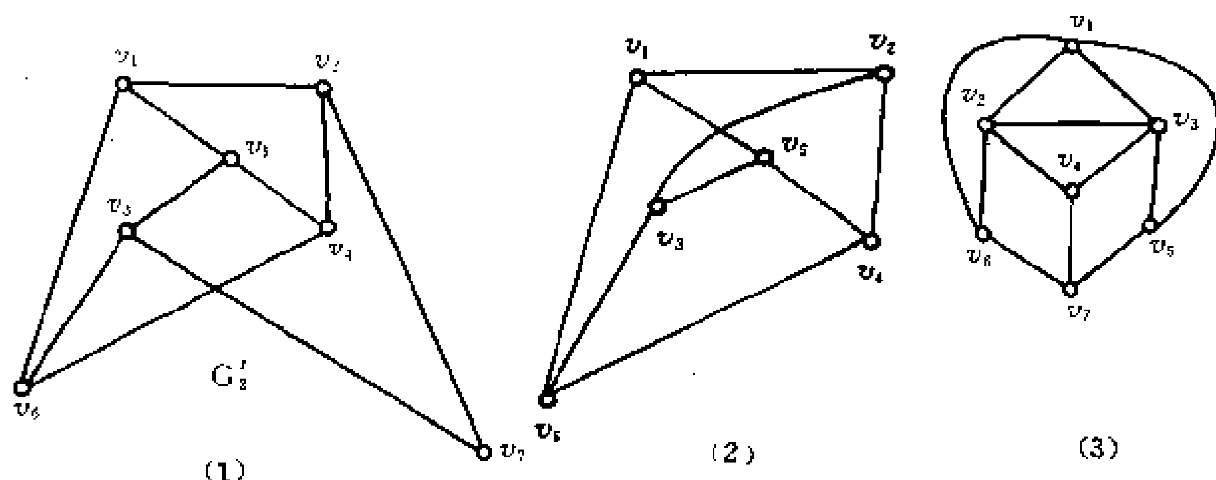


图 8-37

8.3 问答与论证

例 8-40 设连通图 $G=(V,E)$ 是 (n,m) 图，且无环路，则 $m=n-1$.

证 对 G 中结点个数 n 进行归纳证明.

$n=1$ 时，因为 G 无环路

所以 $m=n-1=0$. 结论成立.

设 $n<k$ 时，结论成立，即 $m=n-1$.

当 $n=k$ 时，在 G 中任取一条边 $e=(u,v)$.

因 G 中无环路，

所以 e 不在 G 的任何环路中出现.

故 e 是 G 的割边，则 G-e 含两个分图 G_1，G_2，设 n_1，m_1，n_2，m_2 分别为它们的结点数和边数，且 G_1 和 G_2 无环路，则 $n_1, n_2 < k$，$n_1 + n_2 = n$，$m = m_1 + m_2 + 1$. 由归纳假设知 $m_1 = n_1 - 1$，$m_2 = n_2 - 1$，于是

$$\begin{aligned} m &= m_1 + m_2 + 1 = (n_1 - 1) + (n_2 - 1) + 1 \\ &= (n_1 + n_2) - 1 = n - 1. \end{aligned}$$

因此，由归纳原理知结论成立.

例 8-41 设 $G=(V,E)$ 是一个连通图，$V_1 \subseteq V$，V_1' 是 V_1 相对 V 的补集(即 $V_1' = V - V_1$，亦即 $V_1 \cap V_1' = \varnothing$，$V = V_1 \cup V_1'$)，并且同一结点子集中的任意两个结点之间，至少存在一条不包含另一结点子集中的任何结点的路，那么 G 中端点分别在 V_1 和 V_1' 中的边组成 G 的一个边割集.

证 设 S 是 G 中所有端点分别在 V_1 和 V_1' 中的边的集合，在图 G 中删除 S 中的所有边得图 G-S.

因为 V_1 中任意两结点间有一条不含 V_1' 中结点的路，所以 V_1 中结点与它们在 G-S 中关联的边 E，构成一个连通子图 $G_1 = (V_1, E_1)$. 同理，V_1' 中结点与它们在 G-S 中关联的边 E_2，构成一个连通子图 $G_2 = (V_1', E_2)$.

又因为 $S \subseteq E$ 是 G 中所有一个端点在 V_1，另一端点在 V_1' 中的边集合，所以在 G-S 中，V_1 的任一结点 u 与 V_1' 的任一结点 w 不连接.

从而 G_1，G_2 均是 G-S 的分图，并且当 $S' \subset S$ 时，G-S' 一定连通. 因此，S 是 G 的一个边割集.

例 8-42 若(n,m)图 G 是有 r 个分图的树林，则 $m = n - r$.

证 因为树林的每个分图是树，即 G 的 r 个分图 $G_1, G_2, \cdots, G_r$ 均是树，设 G_i 有 n_i 个结点，m_i 条边($i = 1, 2, \cdots, r$)，则由定理 8.14.1 知 $m_i = n_i - 1$($i = 1, 2, \cdots, r$)，所以

$$\begin{aligned} m &= m_1 + m_2 + \cdots + m_r = (n_1 - 1) + \cdots + (n_r - 1) \\ &= (n_1 + \cdots + n_r) - r = n - r. \end{aligned}$$

例 8-43 试证明若图 G 的每一结点的度为 2，则 G 的每一分图均将包含一环.

证 假设 G 的某一分图 G_k 不含环，且 G_k 为 (n_k, m_k) 图，由条件知 G_k 的每一结点的度数为 2，于是

$$2m_k = \sum_{i=1}^{n_k} \deg(v_i) = 2nk, mk = nk.$$

又 G_k 连通且无环，故是树；由定理 8.14.1 知 $m_k = n_k - 1$ 与 $m_k = n_k$ 矛盾，因此，G 中每个分图必含环.

例 8-44 证明图 G 的任一生成树和任一边割集至少有一条公共边.

证 设图 G 中若有一个边割 S 与 G 的一棵生成树 T 没有公共边，那么删去 S 后所得子图 $G-S$ 必包含 T，这意味着 $G-S$ 仍连通，与 S 是边割集矛盾，所以必是，S 与 T 至少有一条公共边.

例 8-45 连通图 G 的任一边为 G 的某一生成树的弦. 此结论是否正确?

解 若连通图 G 含有割边，则 e 为任何生成树的枝.

若 G 不含割边，那么对 G 的任一边 e'，e' 一定在某个环路 σ 上，用破圈法构成生成树 T_G 时，可在 σ 中删去 e'，相对生成树 T_Ge' 一定是弦.

因此，上述结论当 G 不含割边时才成立.

例 8-46 试证：若 (n, m) 图 G 是二部图，则 $m \leqslant \frac{n^2}{4}$.

证 用反证法 假定 $m > \frac{n^2}{4}$.

设 $G = (V_1, V_2, E)$，$\# V_1 = n_1$，$\# V_2 = n_2$，则 $n = n_1 + n_2$. 由于完全二部图在给定结点集合后具有边数最多，所以 $n_1 \cdot n_2 \geqslant m > \frac{n^2}{4}$. 于是 $4n_1 \cdot n_2 > n^2 = (n_1 + n_2)^2$，即 $2n_1 \cdot n_2 > n_1^2 + n_2^2$.

另一方面 $(n_1 - n_2)^2 \geqslant 0$ 即 $n_1^2 + n_2^2 \geqslant 2n_1 \cdot n_2$ 矛盾所以假设错误，必是 $m \leqslant \frac{n^2}{4}$.

例 8-47　设(n,m)图 G 是连通的平面图，试证明 G 中必有一个结点 v，使得 $\deg(v)\leqslant 5$.

证　用反证法. 设 G 中每个结点的度数$\geqslant 6$，即 $\deg(v_i)\geqslant 6(i=1,2,\cdots,n)$，则由握手定理知

$$2m=\sum_{i=1}^{n}\deg(v_i)\geqslant 6n \quad 即\ n\leqslant\frac{1}{3}m \tag{1}$$

又 G 是连通平面图，且 $\deg(v_i)\geqslant 6$，知 $m\geqslant 2$，由定理 8.20.1 推论知 $m\geqslant 3n-6$. 代入(1)式得 $n\leqslant(n-2)$，矛盾.
所以，G 中至少有一个结点 v，满足 $\deg(v)\leqslant 5$.

例 8-48　试证明 n 阶图 G 中奇次度结点的个数与 $\overline{G}$ 中奇次度结点的个数相等，其中 n 为奇数(度数为奇数的结点，称为奇次度结点).

证　因为 n 为奇数，所以 n 阶完全图 K_n 的每个结点的度数 $n-1$ 为偶数.

设 v 是 G 中任一奇次度结点，$\deg(v)=k$.

在 $\overline{G}$ 中记 $\deg(v)=k'$，则 $k+k'=n-1$，于是 k' 为奇数.

由 v 的任意性知 G 中任一奇次度结点，一定也是$\overline{G}$中奇次度结点. 又 G 与 $\overline{G}$ 互补. 因此，结论成立.

例 8-49　设 G 是(n,m)图，且 $m>\frac{1}{2}(n-1)(n-2)$，则 G 是连通的.

证　用反证法. 假设 G 是不连通的，有 $G_1,\cdots,G_k$ 个连通分图，显然当每个分图均为完全图时，G 的边数最多. 值得注意的是，在 G 中任选取两个分图 K_{n_i}和 $K_{n_j}(n_i\geqslant n_j>1)$，G 的其他分图不变，仅用 K_{n_i+1}和 K_{n_j-1}分别代替 K_{n_i}和 K_{n_j}，所得图与 G 相比较结点数和连通分图数设变，但边数增加了. 因为

$$\left(\frac{1}{2}n_i(n_i+1)+\frac{1}{2}(n_j-1)(n_j-2)\right)$$
$$-\left(\frac{1}{2}n_i(n_i-1)+\frac{1}{2}n_j(n_j-1)\right)$$

$$= n_i - n_j + 1 > 0,$$

所以，G 在一个分图为$(n-(k-1))$阶完全图，其余分图均为一阶完全图的情况下边数最多，此时

$$\text{边数}=\frac{1}{2}(n-(k-1))(n-(k-1)-1)=\frac{1}{2}(n-k)(n-k+1)$$

所以

$m\leqslant\frac{1}{2}(n-k)(n-k+1)$，当 $k\geqslant 2$ 时，

$m\leqslant\frac{1}{2}(n-2)(n-1)$与条件矛盾.

因此，必是 $k=1$，G 是连通的.

例 8-50 证明 对于任何简单图 $G=(V,E)$，或者 G 是连通的，或者 $\overline{G}=(V,\overline{E})$是连通的.

证 若 G 连通，则结论显然成立.

假设 G 不连通，对任意的 $u,v\in V$，若$\{u,v\}\in E$，则显然 u 与 v 在 $\overline{G}$ 中连接.

若$\{u,v\}\notin E$，则由补图的定义知$\{u,v\}\in E$，于是 u,v 属于 G 的同一分图.

又 G 不连通，所以在 G 的另一分图中，存在 $w,w\in V$，使得$\{u,w\}\notin E$ 且$\{v,w\}\notin E$.

因而$\{u,w\}\in E$ 且$\{v,w\}\in E$，u,v 在 $\overline{G}$ 中由 uwv 连接，由 u，v 的任意性知 $\overline{G}$ 是连通的.

例 8-51 证明：若(n,m)图 G 是树，且其最大结点度数 $\Delta(G)=k(\geqslant 2)$，则 G 中至少有 k 片树叶.

证 用反证法. 假设 G 中至多有 $k-1$ 片树叶，则根据握手定理得

$$2m=\sum_{i=1}^{n}\deg(v_i)\geqslant(k-1)+k+2(n-k)=2n-1$$

另一方面由 G 是树得 $m=n-1$，所以 $2n-2\geqslant 2n-1$ 矛盾.

于是假设错误，结论成立.

例 8-52 证明恰有 2 片树叶的树为一条真路.

证 设 T 为恰有 2 片树叶的 (n,m) 树，则由握手定理知

$$2m=\sum_{i=1}^{n}\deg(v_i)=2+\sum_{i=1}^{n-2}\deg(v_i)$$

（其中 v_n,v_{n-1} 为树叶）

另一方面，T 是树，所以 $m=n-1$，于是 $2n-2=2+\sum_{i=1}^{n-2}\deg(v_i)$，即 $\sum_{i=1}^{n-2}\deg(v_i)=2(n-2)$.

由条件知，T 中除 2 个叶结点外，其余 $n-2$ 个分枝结点度数均大于等于 2.

因此，这 $n-2$ 个分枝结点的度数只能都为 2，故 T 有一条欧拉路. 所以 T 为一条真路.

例 8-53 设二部图 $T=(V,E)=(V_1,V_2,E)$ 是一棵树，试证明：若 $\#V_1\geqslant\#V_2$，则在 V_1 中至少有一个度数为 1 的结点.

证 设 $\#V=n,\#E=m,\#V_1=n_1,\#V_2=n_2,S_1=\sum_{v_i\in V_1}\deg(v_i),S_2=\sum_{v_i\in V_2}\deg(v_i)$，则由握手定理知

$$2m=\sum_{v_i\in V_1}\deg(v_i)+\sum_{v_i\in V_2}\deg(v_i).$$

因为 T 是树，所以 $m=n-1$.

又因为 T 是二部图，所以 $S_1=S_2=m$.

假设 V_1 中没有度数为 1 的结点，则 $S_1\geqslant 2n_1$，所以 $2m=S_1+S_2=2S_1\geqslant 2\times 2n_1=4n_1$.

由条件知 $n_1\geqslant n_2$，所以 $2m\geqslant 2n_1+2n_2=2n$，即 $m\geqslant n$ 与 $m=n-1$ 矛盾.

因此，必是 V_1 中至少有一个度为 1 的结点.

例 8-54 若 G 是一个平面图，有 r 个分图，证明 $n-m+k=r+1$，其中 n,m,k 分别为 G 的结点数，边数和面数.

证 设 G 的 r 个分图为 $G_1,G_2,\cdots,G_r$，由于 G 是平面图，所以 G_i 是平面连通图，记 G_i 的结点数、边数、面数分别为 $n_i,m_i,k_i(i=1,2,\cdots,r)$，于是由欧拉公式得

$$n_i - m_i + k_i = 2 \quad (i = 1, 2, \cdots, r). \qquad (1)$$

而 $n = \sum_{i=1}^{r} n_i \quad m = \sum_{i=1}^{r} n_i \quad k = \sum_{i=1}^{r} k_i - (r-1)$（因为每个分图均将无限面记数一次）.

对(1)式两边求和得

$$n - m + k + (r - 1) = 2r, n - m + k = r + 1.$$

注 该式是对欧拉公式的推广.

例 8-55 设(n,m)图 G，是有 r 个分图的平面图，G 的每个面至少由 $l(\geqslant 3)$条边围成，则

$$m \leqslant \frac{l(n-r-1)}{l-2}.$$

证 设 G 有 k 个面，k 个面的各边界长度之和为 S，则 $S \geqslant l \cdot k$.

另一方面，每条边至多在两个面的边界中，所以 $S \leqslant 2m$，于是 $2m \geqslant l \cdot k$，即

$$k \leqslant \frac{2m}{l} \qquad (1)$$

根据欧拉公式的推广（例 8-53）得

$$n - m + k = r + 1 \qquad (2)$$

将(1)代入(2)得 $\quad n - m + \frac{2m}{l} \geqslant r + 1.$

经整理后为 $\quad m \leqslant \frac{l}{l-2}(n - r - 1).$

C. 解题思路与方法

例 C-1 证明：任意 6 个人中，或者有三个人彼此认识或者有三个人彼此陌生.

证 用六个结点 $v_1, v_2, \cdots, v_6$ 分别表示六个人，若 v_i 与 v_j 彼此认识，则用边$\{v_i, v_j\}$连接它们，于是得图 $G=(V,E)$，而在 $\overline{G}=(V,E)$中，边$\{v_i, v_j\}$表示 v_i 与 v_j 彼此陌生. 这样问题转化为证明 G 或 $\overline{G}$ 中存在一个 K_3.

由补图的定义知，完全图 $K_6=G\cup\overline{G}$，在 K_6 中用红色和蓝色分别涂抹 G 中和 $\overline{G}$ 中的边.

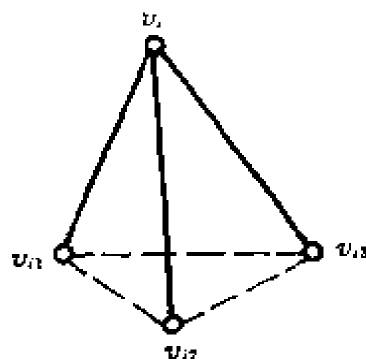


图 C-1

任取 K_6 中一个结点 v_i，则与 v_i 关联的边有 5 条，其中至少有三条边同色，不妨设这三条边为红色，观察这三条边的另一端的三个结点 v_{i1},v_{i2},v_{i3}，若连接这三个结点间的边中有一条为红色，如 $\{v_{i1},v_{i3}\}$，那么 $v_iv_{i1}v_{i3}v_i$ 就是 G 中的一个 K_3. 如图 C-1 所示.

若连接这三个结点间的每条边均为蓝色，那么 $v_{1i}v_{i2}v_{i3}v_{i1}$ 就是 $\overline{G}$ 中的一个 K_3.

因此，或者有三个人彼此认识，或者三个人彼此陌生.

例 C-2 有 n 个人，假定他们中间任意两个人合起来认识其余的 $n-2$ 个人. 证明：$n\geqslant4$ 时，这 n 个人能围着圆桌坐下，使得每个人都认识两旁的人.

解 将每个人用结点表示，有 $V=\{v_1,v_2,\cdots,v_n\}$，若 v_i 与 v_j 认识，则 v_i 与 v_j 邻接，于是得简单无向图 $G=(V,E)$.

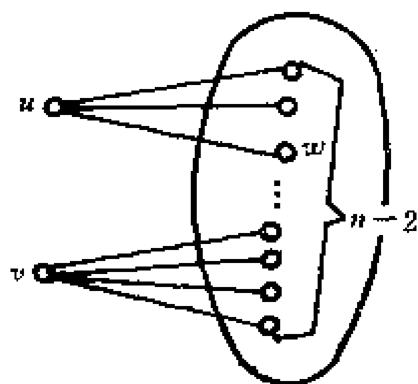


图 C-2

根据条件任意两个人合起来认识其余的 $n-2$ 个人得，对 G 中任意 $u,v\in V$ 有

$$\deg(u)+\deg(v)\geqslant n-2.$$

下面证明当 $n\geqslant4$，u 与 v 不相邻时有 $\deg(u)+\deg(v)\geqslant n$.

当 u 与 v 不邻接时，对任意的 $w\in V$ ($w\neq u,w\neq v$) 由条件知 w 必与 u 和 v 邻接，否则，若 w 仅与 u 邻接，不与 v 邻接，又 u 与 v 不邻接，如图 C-2 所示，u,w 合起来不能保证与其余 $n-2$ 个结点邻接，与条件矛盾.

由 w 的任意性知，其余 $n-2$ 个结点与 u 和 v 均邻接.

于是 $\deg(u)+\deg(v)\geqslant2(n-2)=n+n-4\geqslant n$（当 $n\geqslant$

4 时).

根据定理 8.13.2 的推论 3 知 G 是哈密顿图，有一哈密顿环，于是 n 个人能围圆桌坐下，使每个人都认识两旁的人.

例C-3 证明任一棵树是一个二部图.

证 设 $T=(V,E)$是任一棵树，任取一结点 $v\in V$.

定义 $V_1=\{v_i|v_i\in V$，且 $d(v,v_i)$为偶数$\}$；

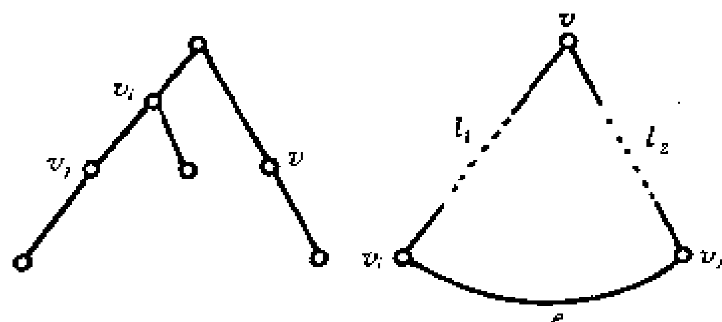


图 C-3

$V_2=V-V_1$，则显然 $V_1\cap V_2=\varnothing$，$V=V_1\cup V_2$.

对 G 的任意一条边 $e=\{v_i,v_j\}\in E$，记 v_i 到 v 的短程为 l_1，v_j 到 v 的短程为 l_2，则 e 在 l_1 上，或者 e 在 l_2 上，否则 $l_1\cup l_2\cup e$ 构成一环路，与 T 是树矛盾. 如图 C-3 所示.

不妨设 e 在 l_2 上，即 v_j 到 v 的短程经过边$\{v_i,v_j\}$，所以

$$d\{v,v_j\}=d(v,v_i)+1.$$

于是 v_i,v_j 不同属于 V_1 或 V_2. 因此，由 e 的任意性得 T 是二部图.

例 C-4 证明：(1)n 阶树 T 的所有结点之和 $\sum_{i=1}^{n}\deg(v_i)=2n-2$；

(2)设 $d_1,d_2,\cdots,d_n$ 是 n 个正整数，$n\geqslant 2$，已知 $\sum_{i=1}^{n}d_i=2n-2$，证明存在结点度数分别为 $d_1,d_2,\cdots,d_n$ 的一棵树.

证 (1)设 $T=(V,E)$，$V=\{v_1,v_2,\cdots,v_n\}$，T 有 m 条边，则由

定理 8.14.1 知 $m=n-1$. 又由握手定理有 $2m=\sum_{i=1}^{n}\deg(v_i)$,所以

$$\sum_{i=1}^{n}\deg(v_i)=2(n-1)=2n-2.$$

(2)对结点 n 归纳证明,可构造满足条件的树 T.

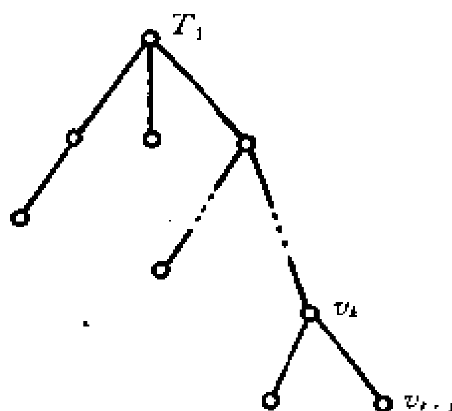


图 C-4

$n=2$ 时,由 $d_1+d_2=4-2=2$,而 $d_1,d_2\geqslant1$,所以 $d_1=d_2=1$. 于是存在 K_2 为满足条件的树.

假设 $n=k$ 时,结论成立,即存在结点度数分别为 $d_1,d_2,\cdots,d_k$ 的一棵树 T_1. 要证 $n=k+1$ 时,结论也成立.

由 $d_1,d_2,\cdots,d_k,d_{k+1}$均为正整数, $\sum_{i=1}^{k+1}d_i=2(k+1)-2=2k$ 知,这 $k+1$ 个数中至少有二个为 1,否则 $\sum_{i=1}^{k+1}d_i\geqslant 2k+1$,与条件矛盾.

不妨设 $d_{k+1}=1$,于是 $\sum_{i=1}^{k}d_i=2k-1$,这样 $d_1,d_2,\cdots,d_k$ 中至少有一个数大于 2,否则 $\sum_{i=1}^{k}d_i\leqslant k$ 矛盾.

不妨设 $d_K\geqslant2$,于是 $d_k-1\geqslant1$.

$$\sum_{i=1}^{k-1}d_i+(d_k-1)=\sum_{i=1}^{k}d_i-1=2k-2.$$

考虑 $d_1,d_2,\cdots,d_{k-1},d_k-1$ 这 k 个正整数,由归纳假设知,存在结点度数分别是 $d_1,d_2,\cdots,d_{k-1},d_K-1$ 的一棵树 T_1.

在 T_1 中从度为 d_k-1 的结点 v_k 引出一条边,另一端点记为 v_{k+1},这样得一棵新树 T,在 T 中 $\deg(v_k)=d_k$,$\deg(v_{k+1})=d_{k+1}=$

1，如图 C-4 所示.

于是 $$\sum_{i=1}^{k+1}\deg(v_i)=\sum_{i=1}^{k+1}d_i=2(k+1)-2.$$

因此，T 即为所求的一棵树.

例 C-5 设 T_1,T_2 是(n,m)连通图 $G=(V,E)$的两棵生成树，a 是在 T_1 中但不在 T_2 中的一条边. 证明存在一条在 T_2 但不在 T_1 中的边 b，使$(T_1-\{a\})\cup\{b\}$和$(T_2-\{b\})\cup\{a\}$都是 G 的生成树.

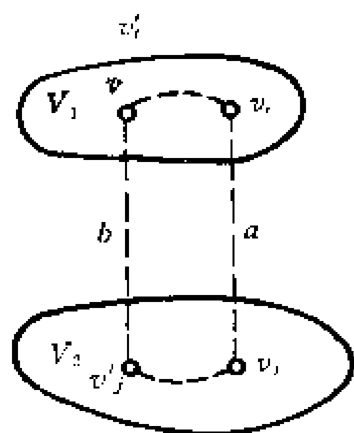


图 C-5

证 记$a=\{v_i,v_j\}$，因为 T 是树，故每条边是割边，所以在 T_1 中去掉边 a，必将把 T_1 分成两棵不连通的子图 T_{11}和 T_{12}，令他们的结点集分别为 V_1,V_2，显然 $V=V_1\cup V_2,V_1\cap V_2=\varnothing$.

T_2 是 G 的另一棵不含 a 的生成树，于是 $T_2\cup\{a\}$恰含一个环 C，在 C 中去掉边 a 后，从 a 的一个端点 $v_i\in V_1$ 出发，沿着 C 寻找一个端点在 V_1 中另一个端点在 V_2 中的边，见图 C-5. 若这样的边不存在，那么 C-$\{a\}$这条真路全在 V_1 中，则$(C-\{a\})\cup\{a\}$不能构成环，(因为 $v_j\in V_2$)，矛盾. 因此，总可找到一条边记作 $b=\{v_i',v_j'\}\in C,b\neq a$，这样的 b 一定不在 T_1 中，否则 $T_1-\{a\}$ 仍连通，与 a 是 T_1 的割边矛盾.

这样，找到边 b 不在 T_1 中，但在 T_2 中，由于 b,a 均在 C 上，故$(T_2-\{b\})\cup\{a\}$是 G 的一棵生成树.

又因为 T_1 是 G 的生成树，含 $n-1$ 条边，所以 $T_3=(T_1-\{a\})\cup\{b\}$也含 $n-1$ 条边，由 b 的选取方式知 T_3 连通且 $m_3=n-1$(m_3 为 T_3 的边数)，故 T_3 是树，所以 T_3 是 G 的生成树.

因此，找到了符合条件的边 b.

例 C-6 设 G 是一个 n 阶图，$n\geqslant 11$，证明 G 与 $\overline{G}$ 中至少有一个是平面图.

证 1)先讨论 $n=11$ 的情况

因为 $K_{11}=G\cup\overline{G}$ 有 $C_{11}^2=\frac{11\times10}{2}=55$ 条边,所以

G 与 $\overline{G}$ 中必有一图的边数 $m\geqslant28$.

不妨设 G 的边数 $m\geqslant28$,下面证 G 是非平面图.

设 G 有 $r(r\geqslant1)$ 个分图,若 G 中不含环路,则 G 必是树或树林,由例 8-42 知 $m=n-r=11-r$,于是 $11-r\geqslant28$ 矛盾,所以 G 必包含有环路.

若 G 是平面图,则其每个面至少由 $l=3$ 条边围成.

由例 8-55 知

$$m\leqslant\frac{l(n-r-1)}{l-2}=\frac{l(11-r-1)}{l-2}$$

$$=\frac{l}{l-2}\times(10-r)\leqslant3(10-r),(\because l\geqslant3,\therefore\frac{l}{l-2}\leqslant3)$$

而 $r\geqslant1$,所以 $m\leqslant3\times9=27$.

与 $m\geqslant28$ 矛盾,因此 G 必是非平面图.

2)若 $n\geqslant11$,则讨论 G 的一个具有 11 个结点的子图 G_1,于是 G_1 或 $\overline{G_1}$ 是非平面图,如果 $\overline{G_1}$ 为非平面图,则 $\overline{G}$ 为非平面图,若 G_1 为非平面图,则 G 为非平面图.

第四部分　数理逻辑

第九章　命题逻辑

9.1　内容提要

1. 命题及其联结词

· 命题、命题的真值；

· 原子命题和复合命题；

· 命题联结词：否定($\neg$)，合取($\wedge$)，析取($\vee$)，异或($\veebar$)，蕴含($\rightarrow$)，等值($\leftrightarrow$)，以及分别由这些联结词构成的复合命题的真值表.

2. 命题公式的有关概念

· 命题常元、命题变元、命题公式(或称公式)；

· 命题公式 F 关于命题变元 $P_1, P_2, \cdots, P_n$ 的一组真值指派，以及公式的真值表；

· 重言式(或永真式)、矛盾式(或永假式)和可满足公式；

· 公式的析取范式和合取范式，以及主析取范式和主合取范式.

3. 命题公式间的关系

· 命题公式间的等值关系($A \Leftrightarrow B$)；

• 命题公式间的蕴含关系($A \Rightarrow B$)；

• 等值定律，即一些基本的等值式；

• 推理定律，即一些基本的蕴含式.

4. 命题演算的推理理论

• 形式证明、有效证明、有效结论、合理证明、合理结论；

• 前提引入规则，结论引入规则，置换规则，代入规则，蕴含证明规则.

9.2 基本知识点

1. 命题的判定

命题是一个能分辨真假的陈述句. 命题的真假用真值描述. 如果一个命题是真的，其真值为真，用"1"表示，否则真值为假，用"0"表示.

例 9-1 判断下列语句是否为命题

(1) 北京是中国的首都；

(2)所有的树木都是植物；

(3)雪是黑色的；

(4)请勿吸烟；

(5)明天开会吗?

(6)这朵花多好看呀!

解 (1)—(3)是命题，其中(1)，(2)是真命题，(3)是假命题；(4)是祈使句，(5)是疑问句，(6)是感叹句，它们都无真假可言，因此，它们都不是命题.

一个语句本身是否能分辨真假与我们是否知道它的真假是两回事. 也就是说，对于一个句子，有时我们可能无法判定它的真假，但它本身却是有真假的，那么这个语句是命题，否则就不是命题.

例 9-2 判断下列语句是否为命题

(1) 地球外的星球上也有人;

(2) 小王是我的同学,也是我的好朋友;

(3) 11+1=100;

(4) 我正在说谎.

解 (1)—(3)是命题.对于(1),目前我们还无法确定其真假,但就事物的本质而论,句子本身是可以分辨真假的.随着科学技术的发展,其真值会知道的.

(2) 的真假取决于“我”与“小王”的关系,若“我”与“小王”是同学,且关系很好,则(2)是真的,否则就是假的.但一般来说,这句话总是出现在某一具体情况下,总可根据当时的情况来确定它的真假.

(3) 的真假取决于采用哪一种进制,若是二进制,则是真的,否则就是假的.

(4) “我”是在说谎还是在说真话呢?如果“我”是说谎,那么“我”说的是假话;因为“我”承认他是说谎,所以他实际上是在说真话,我们得出结论:如果“我”是说谎,那么他是讲真话.另一方面,如果“我”讲真话,那么“我”所说的是真话,也就是他在说谎.我们得出结论:如果“我”讲真话,那么他是在说谎.因此,我们不能分辨这个语句的真假,它不是命题.这种产生自相矛盾的语句叫悖论.

2. 命题联结词及命题的符号化

原子命题 一个不能分解为更简单的命题,称为简单命题或原子命题.

复合命题 由原子命题和联结词复合而成的命题称为复合命题.

将命题符号化的基本步骤如下:

(1) 分析出各原子命题,将它们符号化;

(2) 使用合适的命题联结词,把原子命题逐个联结起来,组成复合命题的符号化表示.

一般来说命题联结词与自然语言中的某些词汇有一定的联系.

“$\neg$”相当于自然语言中的“非”、“不是”或“没有”等否定词.

“$\wedge$”是自然语言中“并且”，“既……又……”，“和”，“以及”，“不仅……而且……”，“虽然……但是……”，“与”等词汇的逻辑抽象.

“$\vee$”与自然语言中的“或”有联系，自然语言中的“或”可表示“可兼或”；$\veebar$表示“不可兼或”.

“$\rightarrow$”是自然语言中的“如果……那么”，“若……则……”，“必须……以便……”等联结词均可用“$\rightarrow$”表示. 另外“$P\rightarrow Q$”还可陈述为：“P 是 Q 的充分条件”，“Q 是 P 的必要条件”，“P 仅当 Q”，“Q 每当 P”.

“$\leftrightarrow$”与自然语言中的“当且仅当”、“相当于”，“……和……一样”，“等价”，“要且仅要”等词汇相对应.

例 9-3 将下列命题符号化.

(1) 小李虽然聪明，但不用功；

(2) 派小王或小李出差；

(3) 小王现在在宿舍或在图书馆里；

(4) 我既不看电视也不外出，我睡觉；

(5) 他钓了 20 或 30 条鱼；

(6) 如果天下大雨，他就乘公共汽车上班；

(7) 只有天下大雨，他才乘公共汽车上班；

(8) n 是偶数当且仅当它能被 2 整除；

(9) 我们不能既走路又划船.

解 (1)令 P：小李聪明。

Q：小李用功. 命题可表示为 $P\wedge\neg Q$.

(2) 令 P：派小王出差；Q：派小李出差.

命题符号化为 $P\vee Q$.

(3)令 P：小王在宿舍；Q：小王在图书馆里.

由于小王不可能既在宿舍又在图书馆，所以这里的“或”是不可兼或，于是命题可表示为$P \bar{\vee} Q$，或者为$(P \wedge \neg Q) \vee (\neg P \wedge Q)$.

(4) 令P：我看电视；Q：我外出；R：我睡觉.

命题可表示为 $\neg P \wedge \neg Q \wedge R$.

(5) 中的“或”是“或许”，“大概”的意思.表示“他大概钓了二、三十条鱼”.此命题不能再分解，故可表示为P，其中P：他钓了20或30条鱼.

(6) 令P：天下大雨；Q：他乘公共汽车上班.

命题可表示为$P \rightarrow Q$.

(7) 令P：天下大雨；Q：他乘公共汽车上班.

“他乘公共汽车上班”的前提条件是天下大雨.命题符号化为$Q \rightarrow P$.

(8)令P：n是偶数；Q：n能被2整除.

该命题符号化为$P \leftrightarrow Q$.

(9) 令P：我们走路；Q：我们划船.

命题可表示为 $\neg(P \wedge Q)$.

需要提醒大家注意的是，自然语言中的联结词与命题联结词的含义不是完全对应的，因此，在将自然语言符号化时，要根据上下文分析，尽量将其含义表示出来.

例9-4 将下列命题符号化.

(1) 王平与李明是好学生；

(2) 王平与李明是好朋友；

(3) 如果我上街，我就去书店看看，除非我很累.

(4) 若不是他生病或出差了，我是不会同意他不参加学习.

解 (1) 令P：王平是好学生；Q：李明是好学生.

命题可表示为$P \wedge Q$.

(2)中的“与”表示的是“王平”、“李明”间的关系，而不是两个命题的联结，所以(2)不能分解成两个命题，只能表示为P.

(3)令P：我上街；Q：我去书店看看；R：我很累.

于是命题中"如果我上街，我就去书店看看"，可以符号化为 $P \to Q$，而联结词"除非……"可以理解为"如果不……"，这样整个句子就可以理解为"如果我不很累，则若我上街，我就去书店看看."因此(3)可以符号化为：$\neg R \to (P \to Q)$. 此句还可理解为："如果我上街并且我没有去书店，那么我一定很累."因而也可符号化为 $(P \wedge \neg Q) \to R$（事实上这两种符号化公式是等值的）.

(4) 令 P：他生病了；Q：他出差了；R：我同意他不参加学习. 这个语句可以理解为："若他生病或出差了，那么我同意他不参加学习，否则，我不会同意他不参加学习". 于是整个句子可符号化为 $((P \vee Q) \to R) \wedge (\neg(P \vee Q) \to \neg R)$，亦即 $(P \vee Q) \leftrightarrow R$.

例 9-5 用日常语言写出一个句子，对应下列每一个命题.

(1) $(\neg P \wedge \neg Q) \to R$；

(2) $R \leftrightarrow (P \vee Q)$.

解 (1) 令 P：明天刮风；Q：明天下雨；R：我们去郊游. 则 $(\neg P \wedge \neg Q) \to R$ 可叙述为"如果明天既不刮风又不下雨，那么我们就去郊游."

(2) 令 P：苹果是甜的；Q：苹果是红的；R：我买苹果. 则 $R \leftrightarrow (P \vee Q)$ 可叙述为"当且仅当苹果是甜的或红的，我才买.

3. 命题公式及其真值指派

命题变元 是一个仅表示任意命题位置的大写字母. 即是一个没有指定具体内容的命题.

命题公式（或简称公式）是 0、1 和命题变元以及由他们与联结词按一定的规则产生的符号串. 递归定义如下：

(1) 0、1 是命题公式；

(2) 命题变元是命题公式；

(3) 如果 A 是命题公式，则 $\neg A$ 是命题公式；

(4) 如果 A 和 B 是命题公式，则 $(A \vee B)$、$(A \wedge B)$，$(A \to B)$，$(A \leftrightarrow B)$ 也是命题公式；

(5) 有限次地利用上述(1)—(4)而产生的符号串是命题公式.

需要指出的是命题公式不是命题,只有当公式中的每一个命题变元都用一个具体的命题代入(或被赋以确定的真值)时,公式的真值才被确定,成为一个命题.

给公式 F 所包含的所有命题变元 $P_1, P_2, \cdots, P_n$ 的一组确定的赋值,称为公式 F 的一组真值指派. 将公式 F 的所有真值指派及其对应的真值用表格的形式表示,那么这样的表格就称为公式 F 的真值表.

例 9-6 下列符号串是否为命题公式,若是,给出其真值表.

(1) $P \to (Q \wedge PR)$;

(2) $(P \vee Q) \to (\neg (Q \wedge R))$.

解 (1)不是命题公式.

(2) 是公式,该公式含三个命题变元,其真值表如表 9-1 所示.

表 9-1

$P\ Q\ R$	$P \vee Q$	$Q \wedge R$	$\neg(Q \wedge R)$	$(P \vee Q) \to (\neg (Q \wedge R))$
0 0 0	0	0	1	1
0 0 1	0	0	1	1
0 1 0	1	0	1	1
0 1 1	1	1	0	0
1 0 0	1	0	1	1
1 0 1	1	0	1	1
1 1 0	1	0	1	1
1 1 1	1	1	0	0

4. 命题公式的类型

命题公式 F,如果对于它所包含的命题变元的任何一组真值指派,取值恒为真,则称公式 F 为重言式,或永真公式,用"1"表示,相反,若对于它所包含的命题变元的任何一组真值指派取值恒为假,则称公式 F 为矛盾式或永假公式. 用"0"表示. 如果至少有

一组真值指派使公式 F 的值为真，则称 F 为可满足的公式.

对一个给定的公式，可用真值表的方法判定它是何种类型的公式.

例 9-7 构造下列命题公式的真值表，并判断它们是何种类型的公式：

(1) $(\neg P \leftrightarrow Q) \leftrightarrow \neg(P \leftrightarrow Q)$；

(2) $(Q \rightarrow P) \wedge (\neg P \wedge Q)$；

(3) $((P \vee Q) \rightarrow (Q \wedge R)) \rightarrow (P \wedge \neg R)$.

解 (1) $F_1 = (\neg P \leftrightarrow Q) \leftrightarrow \neg(P \leftrightarrow Q)$ 的真值表如表 9-2 所示. 由表 9-2 知 F_1 对它的所有真值指派取值恒为真，故是重言式.

(2) $F_2 = (Q \rightarrow P) \wedge (\neg P \wedge Q)$ 的真值表如表 9-2 所示. 由表 9-2 知 F_2 对所有真值指派恒为假，故是矛盾式.

表 9-2

P	Q	$\neg P$	$\neg P \leftrightarrow Q$	$P \leftrightarrow Q$	$\neg(P \leftrightarrow Q)$	F_1	$Q \rightarrow P$	$\neg P \wedge Q$	F_2
0	0	1	0	1	0	1	1	0	0
0	1	1	1	0	1	1	0	1	0
1	0	0	1	0	1	1	1	0	0
1	1	0	0	1	0	1	1	0	0

(3) $F_3 = ((P \vee Q) \rightarrow (Q \wedge R)) \rightarrow (P \wedge \neg R)$ 的真值表如表 9-3 所示，由表 9-3 可知 F_3 是可满足式.

表 9-3

P	Q	R	$\neg R$	$P \vee Q$	$Q \wedge R$	$(P \vee Q) \rightarrow (Q \wedge R)$	$P \wedge \neg R$	F_3
0	0	0	1	0	0	1	0	0
0	0	1	0	0	0	1	0	0
0	1	0	1	1	0	0	0	1
0	1	1	0	1	1	1	0	0
1	0	0	1	1	0	0	1	1
1	0	1	0	1	0	0	0	1
1	1	0	1	1	0	0	1	1
1	1	1	0	1	1	1	0	0

5. 等值式

如果对任何真值指派，公式 A 和公式 B 都有相同的真值，即 $A \leftrightarrow B$ 为重言式，则称 A 和 B 是等值的公式，记作 $A \Leftrightarrow B$，亦即 A 与 B 间有等值关系. 也称 $A \Leftrightarrow B$ 为等值式.

可以验证等值关系是等价关系.

如何判定两个公式是等值式，常用的方法是：真值表方法，等值演算方法.

5.1　真值表方法

例 9-8　判断下列等值式是否成立

(1) $(P \rightarrow Q) \Leftrightarrow (\neg P \rightarrow \neg Q)$；

(2) $P \rightarrow (Q \rightarrow R) \Leftrightarrow (P \wedge Q) \rightarrow R$.

解　(1) 构造公式 $A = P \rightarrow Q$ 与 $B = \neg P \rightarrow \neg Q$ 以及 $A \leftrightarrow B$ 的真值表如表 9-4 所示，由表 9-4 知 $A \leftrightarrow B$ 不是重言式，所以 A 与 B 不等值.

表 9-4

P　Q	$P \rightarrow Q$	$\neg P \rightarrow \neg Q$	$A \leftrightarrow B$
0　0	1	1	1
0　1	1	0	0
1　0	0	1	0
1　1	1	1	1

(2)构造公式 $A = P \rightarrow (Q \rightarrow R)$ 与 $B = (P \wedge Q) \rightarrow R$ 以及 $A \leftrightarrow B$ 的真值表如表 9-5 所示，由于 $A \leftrightarrow B$ 所标记列全为 1，故 $A \leftrightarrow B$ 为重言式，所以 $A \Leftrightarrow B$.

表 9-5

P	Q	R	$Q\to R$	$P\wedge Q$	A	B	$A\leftrightarrow B$
0	0	0	1	0	1	1	1
0	0	1	1	0	1	1	1
0	1	0	0	0	1	1	1
0	1	1	1	0	1	1	1
1	0	0	1	0	1	1	1
1	0	1	1	0	1	1	1
1	1	0	0	1	0	0	1
1	1	1	1	1	1	1	1

5.2　等值演算

等值演算，就是利用已知的一些基本等值式，根据置换和代入规则推导出另外一些等值式的过程. 用等值演算的方法还能化简复杂的公式. 表 9-6 列出了 17 个重要的基本等值式，它们实际上是命题演算的基本定律.

表 9-6

编号	公　式	
E_1	$P\vee Q\Leftrightarrow Q\vee P$	交换律
E_1'	$P\wedge Q\Leftrightarrow Q\wedge P$	
E_2	$(P\vee Q)\vee R\Leftrightarrow P\vee(Q\vee R)$	结合律
E_2'	$(P\wedge Q)\wedge R\Leftrightarrow P\wedge(Q\wedge R)$	
E_3	$P\wedge(Q\vee R)\Leftrightarrow(P\wedge Q)\vee(P\wedge R)$	分配律
E_3'	$P\vee(Q\wedge R)\Leftrightarrow(P\vee Q)\wedge(P\vee R)$	
E_4	$P\vee 0\Leftrightarrow P$	同一律
E_4'	$P\wedge 1\Leftrightarrow P$	
E_5	$P\vee\neg P\Leftrightarrow 1$	互否律
E_5'	$P\wedge\neg P\Leftrightarrow 0$	

续表

编号	公　式
E_6	$\neg(\neg P)\Leftrightarrow P$ 双重否定律
E_7	$P\vee P\Leftrightarrow P$ 等幂律
E_7'	$P\wedge P\Leftrightarrow P$ 等幂律
E_8	$P\vee 1\Leftrightarrow 1$ 零一律
E_8'	$P\wedge 0\Leftrightarrow 0$ 零一律
E_9	$P\vee(P\wedge Q)\Leftrightarrow P$ 吸收律
E_9'	$P\wedge(P\vee Q)\Leftrightarrow P$ 吸收律
E_{10}	$\neg(P\vee Q)\Leftrightarrow\neg P\wedge\neg Q$ 德·摩根定律
E_{10}'	$\neg(P\wedge Q)\Leftrightarrow\neg P\vee\neg Q$ 德·摩根定律
E_{11}	$P\rightarrow Q\Leftrightarrow\neg P\vee Q$
E_{12}	$P\leftrightarrow Q\Leftrightarrow(P\wedge Q)\vee(\neg P\wedge\neg Q)$
E_{13}	$P\rightarrow(Q\rightarrow R)\Leftrightarrow(P\wedge Q)\rightarrow R$
E_{14}	$P\leftrightarrow Q\Leftrightarrow(P\rightarrow Q)\wedge(Q\rightarrow P)$
E_{15}	$P\rightarrow Q\Leftrightarrow\neg Q\rightarrow\neg P$
E_{16}	$\neg(P\leftrightarrow Q)\Leftrightarrow P\leftrightarrow\neg Q$
E_{17}	$\neg(P\rightarrow Q)\Leftrightarrow P\wedge\neg Q$

例 9-9　证明下列命题公式的等值关系：

(1) $(P\rightarrow Q)\wedge(R\rightarrow Q)\Leftrightarrow(P\vee R)\rightarrow Q$；

(2) $P\Leftrightarrow(P\wedge Q)\vee(P\wedge\neg Q)$；

(3) $((Q\wedge R)\rightarrow S)\wedge(R\rightarrow(P\vee S))\Leftrightarrow(R\wedge(P\rightarrow Q))\rightarrow S$.

分析　证明两个公式等值可以从其中任一个开始进行等值演算，一般从较复杂的公式开始，也可以对两个公式 A 和 B 分别进行等值推演，如果能将 A 和 B 都等值推演为同一个公式，那么由等值关系的传递性即可知 $A\Leftrightarrow B$.

证(1) ∵ $(P\rightarrow Q)\wedge(R\rightarrow Q)$

$\Leftrightarrow(\neg P\vee Q)\wedge(\neg R\vee Q)$　　E_{11}

$\Leftrightarrow(\neg P\wedge\neg R)\vee Q$　　E_3(分配律)

$\Leftrightarrow\neg(P\vee R)\vee Q$　　E_{10}(德·摩根律)

$\Leftrightarrow(P\vee R)\rightarrow Q$　　E_{11}

$\therefore (P\to Q)\wedge(R\to Q)\Leftrightarrow(P\vee R)\to Q$

(2) $\because (P\wedge Q)\vee(P\wedge\neg Q)$

$\Leftrightarrow P\wedge(Q\vee\neg Q)$ E_3(分配律)

$\Leftrightarrow P\wedge 1$ E_5(互否律)

$\Leftrightarrow P$ $E_4{}'$(同一律)

$\therefore P\Leftrightarrow(P\wedge Q)\vee(P\wedge\neg Q)$

(3) $\because ((Q\wedge R)\to S)\wedge(R\to(P\vee S))$

$\Leftrightarrow(\neg(Q\wedge R)\vee S)\wedge((\neg R\vee P)\vee S)$ E_{11},E_2

$\Leftrightarrow((\neg Q\vee\neg R)\wedge(\neg R\vee P))\vee S$ $E_{10}{}',E_3$

$\Leftrightarrow(\neg R\vee(\neg Q\wedge P))\vee S$ E_1,E_3,E_2

又$\because$右式$=(R\wedge(P\to Q))\to S$

$\Leftrightarrow\neg(R\wedge(\neg P\vee Q))\vee S$ E_{11}

$\Leftrightarrow(\neg R\vee(\neg(\neg P)\wedge\neg Q))\vee S$ $E_{10}{}',E_{10}$

(德·摩根定律)

$\Leftrightarrow(\neg R\vee(\neg Q\wedge P))\vee S$ E_6,E_1

$\therefore ((Q\wedge R)\to S)\wedge(R\to(P\vee S))\Leftrightarrow(R\wedge(P\to Q))\to S$

例 9-10 化简公式$((\neg P\to\neg P)\to Q)\to((\neg P\to\neg P)\to R)$

解 原式$\Leftrightarrow(\neg(\neg(\neg P)\vee\neg P)\vee Q)\to(\neg(\neg(\neg P)\vee\neg P)\vee R)$ E_{11}

$\Leftrightarrow\neg(\neg(P\vee\neg P)\vee Q)\vee(\neg(P\vee\neg P)\vee R)$ E_6,E_{11}

$\Leftrightarrow((P\vee\neg P)\wedge\neg Q)\vee(\neg(P\vee\neg P)\vee R)$ E_{10},E_6

$\Leftrightarrow(1\wedge\neg Q)\vee(0\vee R)$ E_5

$\Leftrightarrow\neg Q\vee R.$ $E_4,E_4{}'$

另外,用等值演算的方法可以判别命题公式的类型.

例 9-11 判别下列公式的类型:

(1) $Q\wedge\neg(\neg P\to(\neg P\wedge Q))$;

(2) $(P\to Q)\wedge\neg P$.

解 (1) $\because Q\wedge\neg(\neg P\to(\neg P\wedge Q))$

$\Leftrightarrow Q\wedge\neg(P\vee(\neg P\wedge Q))$ E_{11},E_6

$\Leftrightarrow Q\wedge\neg((P\vee\neg P)\wedge(P\vee Q))$ E_3'

$\Leftrightarrow Q\wedge\neg(1\wedge(P\vee Q))$ E_5

$\Leftrightarrow Q\wedge\neg P\wedge\neg Q$ E_4'，E_{10}

$\Leftrightarrow\neg P\wedge(Q\wedge\neg Q)$ E_1'，E_2'

$\Leftrightarrow 0$ E_5'，E_8'

$\therefore Q\wedge\neg(\neg P\rightarrow(\neg P\wedge Q))$是矛盾式.

(2) $\because (P\rightarrow Q)\wedge\neg P$

$\Leftrightarrow(\neg P\vee Q)\wedge\neg P$ E_{11}

$\Leftrightarrow\neg P$ E_9'（吸收律）

而(0,1)是使公式$(P\rightarrow Q)\wedge\neg P$取值为真的真值指派(其中(0,1)表示$P$,$Q$的取值分别为0和1). 于是该公式是可满足式.

6. 蕴含式

设A、B是两个公式，若公式$A\rightarrow B$是重言式，即$A\rightarrow B\Leftrightarrow 1$，则称公式$A$蕴含公式$B$，记为$A\Rightarrow B$，亦即$A$与$B$间有蕴含关系. 也称"$A\Rightarrow B$"为蕴含式.

可验证蕴含关系是偏序关系.

给定两个公式A、B，如何判定蕴含式$A\Rightarrow B$是否成立？根据蕴含式的定义，上述问题转化为判定$A\rightarrow B$是否为重言式，这样，可得下述判定方法：

(1) 直接用真值表证明$A\rightarrow B\Leftrightarrow 1$；

(2) 由等值演算证明$A\rightarrow B\Leftrightarrow 1$；

(3) 假定前件A为真，检查在此情况下，其后件B是否也为真. 这是因为要判定$A\rightarrow B$是否为重言式，由联结词"$\rightarrow$"的真值表知，只需判定其真值表中第三行的情况是否发生. 因此，若在假定前件A真的情况下，能说明后件B一定也真，则可知真值表中第三行的情况不会发生，故$A\rightarrow B$是重言式，所以$A\Rightarrow B$；

A	B	$A\rightarrow B$
0	0	1
0	1	1
1	0	0
1	1	1

(4) 假定后件 B 为假，检查在此情况下，其前件 A 是否也假，若能说明前件不可能为真，则 $A \Rightarrow B$，否则，该蕴含式不成立. 理由同(3).

例 9-12 证明 $((P \vee Q) \wedge (P \rightarrow R) \wedge (Q \rightarrow R)) \Rightarrow R$

证 方法一 列公式 $F_1 = ((P \vee Q) \wedge (P \rightarrow R) \wedge (Q \rightarrow R)) \rightarrow R$ 的真值表如表 9-7 所示.

表 9-7

P	Q	R	$P \vee Q$	$P \rightarrow R$	$Q \rightarrow R$	$(P \vee Q) \wedge (P \rightarrow R) \wedge (Q \rightarrow R)$	F_1
0	0	0	0	1	1	0	1
0	0	1	0	1	1	0	1
0	1	0	1	1	0	0	1
0	1	1	1	1	1	1	1
1	0	0	1	0	1	0	1
1	0	1	1	1	1	1	1
1	1	0	1	0	0	0	1
1	1	1	1	1	1	1	1

由表 9-7 知公式 F_1 对任意的一组真值指派取值均为 1，故 F_1 是重言式.

方法二 $\because ((P \vee Q) \wedge (P \rightarrow R) \wedge (Q \rightarrow R)) \rightarrow R$

$\Leftrightarrow \neg((P \vee Q) \wedge (\neg P \vee R) \wedge (\neg Q \vee R)) \vee R \qquad E_{11}$

$\Leftrightarrow \neg((P \vee Q) \wedge ((\neg P \wedge \neg Q) \vee R)) \vee R \qquad E_3'$

$\Leftrightarrow (\neg(P \vee Q) \vee \neg(\neg(P \vee Q) \vee R)) \vee R \qquad E_{10}, E_{10}'$

$\Leftrightarrow (\neg(P \vee Q) \vee ((P \vee Q) \wedge \neg R)) \vee R \qquad E_6, E_{10}$

$\Leftrightarrow ((\neg(P \vee Q) \vee (P \vee Q)) \wedge (\neg(P \vee Q) \vee \neg R)) \vee R \quad E_3'$

$\Leftrightarrow (1 \wedge (\neg(P \vee Q) \vee \neg R)) \vee R \qquad E_5$

$\Leftrightarrow \neg(P \vee Q) \vee (\neg R \vee R)$ 　　E_4'，E_2

$\Leftrightarrow \neg(P \vee Q) \vee 1$ 　　E_5

$\Leftrightarrow 1$ 　　E_8

$\therefore (P \vee Q) \wedge (P \to R) \wedge (Q \to R) \Rightarrow R$.

方法三 假定蕴含式的前件$(P \vee Q) \wedge (P \to R) \wedge (Q \to R)$为真，则$(P \vee Q)$、$(P \to R)$、$(Q \to R)$分别为真. 由 $P \vee Q$ 真，可得 P 真或 Q 为真，分情况讨论：

(1) 若 P 为真，则由 $P \to R$ 为真，得 R 为真；

(2) 若 Q 为真，则由 $Q \to R$ 为真，得 R 为真.

因此，假定前件$(P \vee Q) \wedge (P \to R) \wedge (Q \to R)$为真时，可推断出后件 R 也为真，故$(P \vee Q) \wedge (P \to R) \wedge (Q \to R) \Rightarrow R$.

用真值表和等值演算的方法证明蕴含式有时较繁，但使用前面介绍的(3)，(4)方法时，要根据具体的公式选择用(3)或(4)，如下例中用方法(4)比方法(3)简单.

例 9-13 证明：$P \to (Q \to R) \Rightarrow (P \to Q) \to (P \to R)$.

方法一 假定 $P \to (Q \to R)$为真，此时不能确定 P，Q，R 的真值，故分情况讨论.

(1) 假定 P 真，则 $Q \to R$ 为真. 若 Q 为真，则 R 必为真，从而 $P \to Q$ 和 $P \to R$ 均为真，因此$(P \to Q) \to (P \to R)$为真；

若 Q 为假，则 $P \to Q$ 为假，从而$(P \to Q) \to (P \to R)$为真.

(2) 假定 P 假，则 $P \to Q$ 为真，$P \to R$ 也为真，所以$(P \to Q) \to (P \to R)$为真.

由(1)，(2)知，当 $P \to (Q \to R)$为真时，$(P \to Q) \to (P \to R)$一定为真，因此 $P \to (Q \to R) \Rightarrow (P \to Q) \to (P \to R)$.

方法二 假定$(P \to Q) \to (P \to R)$为假，则 $P \to Q$ 为真，且 $P \to R$ 为假，由 $P \to R$ 为假得 P 为真，R 为假，再由 P 和 $P \to Q$ 为真，得 Q 也为真，所以 $Q \to R$ 为假，从而 $P \to (Q \to R)$为假，因此 $P \to (Q \to R) \Rightarrow (P \to Q) \to (P \to R)$.

7. 等值关系与蕴含关系的区别与联系

对任意的公式 A、B，若 $A \Leftrightarrow B$，则一定有 $A \Rightarrow B$，反之则不一定成立. 但是，若 $A \Rightarrow B$ 且 $B \Rightarrow A$，则 $A \Leftrightarrow B$.

等值关系是一等价关系，蕴含关系是一偏序关系.

例 9-14 对任意的公式 A,B,

(1) 如果 $A \Leftrightarrow B$，是否有 $\neg A \Leftrightarrow \neg B$?

(2) 如果 $A \Rightarrow B$，是否有 $\neg A \Rightarrow \neg B$?

解 (1)设 $P_1, P_2, \cdots, P_n$ 是公式 A 和 B 中出现的全部命题变元，显然，$\neg A$，$\neg B$ 中所出现的全部命题变元也包含在 $P_1, P_2, \cdots, P_n$ 中. 由于 $A \Leftrightarrow B$，所以对于 $P_1, P_2, \cdots, P_n$ 的任意一组真值指派，A 与 B 的取值均相同，于是 $\neg A$ 与 $\neg B$ 的取值也必然相同. 因此，由定义知 $\neg A \Leftrightarrow \neg B$.

(2) 不一定有 $\neg A \Rightarrow \neg B$ 成立，例如令 $A = P \wedge Q$，$B = P$，可以验证 $P \wedge Q \rightarrow P$ 为重言式，则 $P \wedge Q \Rightarrow P$，但 $\neg(P \wedge Q) \rightarrow \neg P$ 不是重言. 因为当 P 为真，Q 为假时，$\neg(P \wedge Q)$ 为真，而 $\neg P$ 为假，所以 $\neg(P \wedge Q) \not\Rightarrow \neg P$，即 $\neg A \Rightarrow \neg B$ 不成立.

8. 形式证明中的直接证明方法

设 $H_1, H_2, \cdots, H_n$ 和 C 是一些命题公式，若蕴含式

$$H_1 \wedge H_2 \wedge \cdots \wedge H_n \Rightarrow C \qquad (*)$$

成立，则称 C 是前提集合 $\{H_1, H_2, \cdots, H_n\}$ 的有效结论，或称从前提 $H_1, H_2, \cdots, H_n$ 能推出有效结论 C. 有时也记作

$H_1, H_2, \cdots, H_n \Rightarrow C$.

证明蕴含式(*)的形式证明是一个命题公式序列，这个序列的最后一个公式是 C，而前面的公式或者为 $H_1, H_2, \cdots, H_n$ 之一，或者为 $H_1, H_2, \cdots, H_n$ 中的某些公式所推得的结论.

形式证明中的直接证法，则是由一组前提，利用推理规则，根据已知的蕴含式和等值式推导出有效结论的方法.

常用的推理规则如下：

(1) 前提引入规则：在证明的任何步骤上都可以引用前提；

(2) 结论引用规则：在证明的任何步骤上所得到的结论都可以在其后的证明中引用；

(3) 置换规则：在证明的任何步骤上，命题公式的子公式都可以用与之等值的其他命题公式置换.

(4) 代入规则：在证明的任何步骤上，重言式中的任一命题变元，都可以用一命题公式代入，得到的仍是重言式；

(5) 蕴含证明规则：如果能够从 Q 和前提集合 P 中推导出 R 来，则就能从 P 中推导出 $Q \rightarrow R$ 来. 该规则也称为 CP 规则.

在推理中常用的基本蕴含式如表 9-8 所示.

表 9-8

编　号	公　　式
I_1	$P \wedge Q \Rightarrow P$
I_2	$P \wedge Q \Rightarrow Q$
I_3	$P \Rightarrow P \vee Q$
I_4	$Q \Rightarrow P \vee Q$
I_5	$\neg P \Rightarrow P \rightarrow Q$
I_6	$Q \Rightarrow P \rightarrow Q$
I_7	$\neg(P \rightarrow Q) \Rightarrow P$
I_8	$\neg(P \rightarrow Q) \Rightarrow \neg Q$
I_9	$P, Q \Rightarrow P \wedge Q$
I_{10}	$\neg P, P \vee Q \Rightarrow Q$
I_{11}	$P, P \rightarrow Q \Rightarrow Q$
I_{12}	$\neg Q, P \rightarrow Q \Rightarrow \neg P$
I_{13}	$P \rightarrow Q, Q \rightarrow R \Rightarrow P \rightarrow R$
I_{14}	$P \vee Q, P \rightarrow R, Q \rightarrow R \Rightarrow R$

例 9-15 形式证明$\neg S$是$P \to Q$,$(\neg Q \vee R) \wedge \neg R$,$\neg(\neg P \wedge S)$的有效结论.

分析 由于前提公式$\neg(\neg P \wedge S)$中包含有结论$\neg S$,因此,从它着手,可得$P \vee \neg S$,再根据I_{10}消去P,即可得$\neg S$.

证

编 号	公 式	依 据
(1)	$\neg(\neg P \wedge S)$	前提(前提引入规则)
(2)	$P \vee \neg S$	(1);E_{10}',E_6
(3)	$(\neg Q \vee R) \wedge \neg R$	前提
(4)	$\neg Q \vee R$	(3);I_1(用代入规则)
(5)	$\neg R$	(3);I_2
(6)	$\neg Q$	(4),(5);I_{10}(用结论引入规则)
(7)	$P \to Q$	前提
(8)	$\neg P$	(6),(7);I_{12}
(9)	$\neg S$	(2),(8);I_{10}

例 9-16 证明$P \wedge Q$,$(P \leftrightarrow Q) \to (R \vee S) \Rightarrow R \vee S$.

分析 公式$(P \leftrightarrow Q) \to (R \vee S)$的后件是我们要证的结论,若能证得$P \leftrightarrow Q$,由$I_{11}$就可得结论$R \vee S$,因此,想到由$P \wedge Q$证$P \leftrightarrow Q$,而$P \leftrightarrow Q \Leftrightarrow (P \wedge Q) \vee (\neg P \wedge \neg Q) E_{12}$.

证

编 号	公 式	依 据
(1)	$P \wedge Q$	前提
(2)	$(P \wedge Q) \vee (\neg P \vee \neg Q)$	(1);I_3
(3)	$P \leftrightarrow Q$	(2);E_{12}
(4)	$(P \leftrightarrow Q) \to (R \vee S)$	前提
(5)	$R \vee S$	(3),(4);I_{11}

例 9-17 形式证明 $S \to \neg Q$ 是 $\neg P \vee \neg Q, \neg P \to R, R \to \neg S$ 的有效结论.

分析 要证的结论是一个含蕴含联结词的公式,因此,很容易想到采用蕴含证明规则证.

证

编号	公式	依据
(1)	$\neg P \to R$	前提
(2)	$R \to \neg S$	前提
(3)	$\neg P \to \neg S$	(1),(2);I_{13}
(4)	$S \to P$	(3);E_{15}
(5)	S	附加前提
(6)	P	(4),(5);I_{11}
(7)	$\neg P \vee \neg Q$	前提
(8)	$\neg Q$	(6),(7);I_{10}
(9)	$S \to \neg Q$	(5),(8);CP 规则

需要指出的是,使用蕴含规则(即 CP 规则)进行推理时,好像多了一个条件,推演起来可能方便些,但任何事情都不是绝对的,要视情况而定.如例 9-17 不采用蕴含式证明规则时,可简化二步.而例 9-25 若不使用该规则,则不易着手推理.

例 9-17 的另一证明:

编号	公式	依据
(1)	$\neg P \to R$	前提
(2)	$R \to \neg S$	前提
(3)	$\neg P \to \neg S$	(1),(2);I_{13}
(4)	$\neg P \vee \neg Q$	前提
(5)	$Q \to \neg P$	(4);E_1,E_{11}
(6)	$Q \to \neg S$	(3),(5);I_{13}
(7)	$S \to \neg Q$	(6);E_{15}

9. 形式证明中的间接证明方法

间接证明法也就是大家熟悉的反证法.把结论的否定作为假

设(即附加前提),与给定的前提一起作为前提集合进行推证,若能推导出矛盾,则结论是有效结论. 即是若

$$(H_1 \wedge \cdots \wedge H_n) \wedge \neg C \Rightarrow R \wedge \neg R,$$

则

$$H_1 \wedge \cdots \wedge H_n \Rightarrow C$$

其中 C 是要由前提集合 $\{H_1, H_2, \cdots, H_n\}$ 推出的结论,R 为任一公式.

例 9-18 试证 $\neg S$ 是 $P \rightarrow (\neg Q \rightarrow R), Q \rightarrow \neg P, S \rightarrow \neg R, P$ 的有效结论.

分析 用反证法,将 $\neg(\neg S)$ 作为附加前提,添加到前提集合中,然后推导出矛盾.

证

编 号	公 式	依 据
(1)	$\neg(\neg S)$	附加前提
(2)	S	(1);E
(3)	$S \rightarrow \neg R$	前提
(4)	$\neg R$	(2),(3);I_{11}
(5)	$P \rightarrow (\neg Q \rightarrow R)$	前提
(6)	P	前提
(7)	$\neg Q \rightarrow R$	(5),(6);I_{11}
(8)	Q	(4),(7);I_{12},E_6
(9)	$Q \rightarrow \neg P$	前提
(10)	$\neg P$	(8),(9);I_{11}
(11)	$P \wedge \neg P$	(4),(10);I_9

所以 $P \rightarrow (\neg Q \rightarrow R), Q \rightarrow \neg P, S \rightarrow \neg R, P \Rightarrow \neg S$.

注意 采用间接证明方法与使用蕴含规则一样,好像增加了一个条件,即结论的否定公式,但在推理证明中,采用什么方法简

单些，要视情况而定．如例 9-18 中不用间接证法也行，两者的繁简程度差不多．

例 9-18 的另一证明

编　号	公　　式	依　　据
(1)	$P\rightarrow(\neg Q\rightarrow R)$	前提
(2)	P	前提
(3)	$\neg Q\rightarrow R$	(1)，(2)；I_{11}
(4)	$Q\rightarrow\neg P$	前提
(5)	$\neg Q$	(2)；E_6，I_{12}
(6)	R	(5)，(3)；I_{11}
(7)	$S\rightarrow\neg R$	前提
(8)	$\neg(\neg R)$	(6)；E_6
(9)	$\neg S$	(8)，(7)；I_{12}

10. 范式

由若干个命题变元或命题变元的否定构成的合取式称为质合取式，即 $A=P_1^*\wedge P_2^*\wedge\cdots\wedge P_n^*$ 为质合取式，其中 P_i^* 为 P_i 或 $\neg P_i$，P_i 是命题变元．$(i=1,2,\cdots,n)$．

由若干个质合取式的析取构成的公式，称为析取范式．即该公式具有形式 $A_1\vee A_2\vee\cdots\vee A_r(r\geqslant1)$，其中 $A_i(i=1,2,\cdots,r)$都是质合取式．

由若干个命题变元或命题变元的否定构成的析取式称为质析取式．即 $A=P_1^*\vee P_2^*\vee\cdots\vee P_n^*$ 为质析取式，其中 P_i^* 为 P_i 或 $\neg P_i$，$P_i(i=1,2,\cdots,n)$是命题变元．

由若干个质析取式的合取构成的公式称为合取范式．即该公式具有形式 $A_1\wedge A_2\wedge\cdots\wedge A_r(r\geqslant1)$，其中 $A_i(i=1,2,\cdots,r)$都是质析取式．

任何一个命题公式都可以变换为与它等值的析取范式和合取范式，其步骤如下：

(1) 利用 E_{11} 和 E_{12} 消去公式中的运算"$\rightarrow$"和"$\leftrightarrow$";

(2) 利用 E_{10} 和 E_{11} 将公式中出现的"$\neg$"向内深入,使之只作用于命题变元;

(3) 利用双重否定律(E_6)将 $\neg(\neg P)$ 置换成 P;

(4) 利用分配律将公式变为所需要的范式.

例 9-19 求 $(P\rightarrow(Q\wedge R))\wedge(\neg P\rightarrow(\neg Q\wedge\neg R))$ 的析取范式和合取范式.

解 (一)求析取范式

$(P\rightarrow(Q\wedge R))\wedge(\neg P\rightarrow(\neg Q\wedge\neg R))$

$\Leftrightarrow(\neg P\vee(Q\wedge R))\wedge(\neg(\neg P)\vee(\neg Q\wedge\neg R))$ $\qquad E_{11}$

$\Leftrightarrow(\neg P\vee(Q\wedge R))\wedge(P\vee(\neg Q\wedge\neg R))$ $\qquad E_6$

$\Leftrightarrow[(\neg P\vee(Q\wedge R))\wedge P]\vee[(\neg P\vee(Q\wedge R))$
$\quad\wedge(\neg Q\wedge\neg R)]$ $\qquad E_3$

$\Leftrightarrow(\neg P\wedge P)\vee(P\wedge Q\wedge R)\vee(\neg P\wedge\neg Q\wedge\neg R)$
$\quad\vee(Q\wedge R\wedge\neg R\wedge\neg Q)$ $\qquad E_3$

$\Leftrightarrow O\vee(P\wedge Q\wedge R)\vee(\neg P\wedge\neg Q\wedge\neg R)\vee O$ $\qquad E_5'$

$\Leftrightarrow(P\wedge Q\wedge R)\vee(\neg P\wedge\neg Q\wedge\neg R)$ $\qquad E_4$

(二)求合取范式

$(P\rightarrow(Q\wedge R))\wedge(\neg P\rightarrow(\neg Q\wedge\neg R))$

$\Leftrightarrow(\neg P\vee(Q\wedge R))\wedge(\neg(\neg P)\vee(\neg Q\wedge\neg R))$ $\qquad E_{11}$

$\Leftrightarrow(\neg P\vee(Q\wedge R))\wedge(P\vee(\neg Q\wedge\neg R))$ $\qquad E_6$

$\Leftrightarrow(\neg P\vee Q)\wedge(\neg P\vee R)\wedge(P\vee\neg Q)\wedge(P\vee\neg R)$ $\qquad E_3$

给定命题变元 $P_1,P_2,\cdots,P_n$,由 P_i 或 $\neg P_i(i=1,2,\cdots,n)$ 构成的合取公式 $\bigwedge\limits_{i=1}^{n}P_i^*$ 称为由命题变元 $P_1,P_2,\cdots,P_n$ 所产生的最小项,而形如 $\bigvee\limits_{i=1}^{n}P_i^*$ 的命题公式称为由命题变元 $P_1,P_2,\cdots,P_n$ 所产生的最大项. 其中,每一个 P_i^* 为 P_i 或者为 $\neg P_i$. 由不同最小项所构成的析取式,称为主析取式. 由不同最大项所构成的合取式称为主合取范式.

例 9-20 求公式 $P\rightarrow(P\wedge(Q\rightarrow P))$ 的主析取范式及主合取范式，并判定公式类型.

解 (1)求主析取范式

$P\rightarrow(P\wedge(Q\rightarrow P))$

$\Leftrightarrow\neg P\vee(P\wedge(\neg Q\vee P))$ $\quad E_{11}$

$\Leftrightarrow\neg P\vee(P\wedge\neg Q)\vee P$ $\quad E_3, E_7'$

$\Leftrightarrow(\neg P\wedge(Q\vee\neg Q))\vee(P\wedge\neg Q)$

$\quad\vee(P\wedge(Q\vee\neg Q))$ $\quad E_4', E_5$

$\Leftrightarrow(\neg P\wedge Q)\vee(\neg P\wedge\neg Q)\vee(P\wedge\neg Q)$

$\quad\vee(P\wedge Q)\vee(P\wedge\neg Q)$ $\quad E_3$

$\Leftrightarrow(P\wedge Q)\vee(\neg P\wedge\neg Q)\vee(\neg P\wedge Q)\vee(P\wedge\neg Q)$ $\quad E_1, E_7$

由于公式的主析取范式包含了所有的最小项，因此原公式为重言式.

(2)求主合取范式

$P\rightarrow(P\wedge(Q\rightarrow P))$

$\Leftrightarrow\neg P\vee(P\wedge(\neg Q\vee P))$ $\quad E_{11}$

$\Leftrightarrow(\neg P\vee P)\wedge(\neg P\vee\neg Q\vee P)$ $\quad E_3'$

$\Leftrightarrow 1\wedge 1$ $\quad E_5, E_1$

$\Leftrightarrow 1$

由于所得的主合取范式是一空公式，因此原公式为重言式.

说明 用主范式判定一个公式的类型时，只需求出公式的任一种主范式，如果这个主范式为空公式，则由空公式是 0 还是 1，立即可知公式是矛盾式，还是重言式；如果主范式不是空公式，则看它是否有 2^n 项，如果有 2^n 项且是主析取范式，即可知公式是重言式；如果有 2^n 项且是主合取范式，即可知公式是矛盾式；如果主范式即非空公式又未包含 2^n 项，则必为可满足式.

9.3 问答与论证

例 9-21 试证 $\neg B$ 是 $\neg B\vee D$，$(E\rightarrow\neg F)\rightarrow\neg D$，$\neg E$ 的有效

结论.

分析 $\neg B$ 是前提公式 $\neg B \vee D$ 的一析取项，又 $\neg E$ 既不是公式 $(E \to \neg F) \to \neg D$ 的前件，也不是其后件的非，因此，用直接证法不易着手推证，故采用间接证法.

证

编号	公式	依据
(1)	$\neg(\neg B)$	附加前提
(2)	$\neg B \vee D$	前提
(3)	D	(1),(2); I_{10}
(4)	$(E \to \neg F) \to \neg D$	前提
(5)	$\neg(E \to \neg F)$	(3),(4); E_6, I_{12}
(6)	$\neg(\neg E \vee \neg F)$	(5); E_{11}
(7)	$E \wedge F$	(6); E_{10}
(8)	E	(7); I_1
(9)	$\neg E$	前提
(10)	$E \wedge \neg E$	(8),(9); I_9

所以 $\neg B \vee D, (E \to \neg F) \to \neg D, \neg E \Rightarrow \neg B$.

例 9-22 用两种以上方法证明

$$(P \to Q) \to R \Rightarrow (R \to P) \to (S \to P).$$

证法一 $((P \to Q) \to R) \to ((R \to P) \to (S \to P))$

$\Leftrightarrow \neg(\neg(\neg P \vee Q) \vee R) \vee (\neg(\neg R \vee P) \vee (\neg S \vee P))$ E_{11}

$\Leftrightarrow ((\neg P \vee Q) \wedge \neg R) \vee (R \wedge \neg P) \vee (\neg S \vee P)$ E_6, E_{10}

$\Leftrightarrow [((\neg P \vee Q) \vee (R \wedge \neg P)) \wedge (\neg R \vee (R \wedge \neg P))]$
$\vee (\neg S \vee P)$ E_3'

$\Leftrightarrow [(Q \vee (\neg P \vee (R \wedge \neg P))) \wedge (\neg R \vee R) \wedge (\neg R \vee \neg P)]$
$\vee (\neg S \vee P)$ E_1, E_2, E_3'

$\Leftrightarrow [(Q \vee \neg P) \wedge (\neg R \vee \neg P)] \vee (\neg S \vee P)$ E_9, E_5, E_4'

$\Leftrightarrow (Q \wedge \neg R) \vee \neg P \vee (\neg S \vee P)$ E_3'

$\Leftrightarrow (Q \wedge \neg R) \vee (\neg P \vee P) \vee \neg S$ E_1, E_2

$\Leftrightarrow 1$　　E_5, E_8

证法二　假定后件$(R\rightarrow P)\rightarrow(S\rightarrow P)$为假，则$(R\rightarrow P)$为真且$(S\rightarrow P)$为假，由$S\rightarrow P$为假得$S$为真，$P$为假，再根据$R\rightarrow P$为真可得$R$为假，于是$P\rightarrow Q$为真，$(P\rightarrow Q)\rightarrow R$为假，因此，$(P\rightarrow Q)\rightarrow R\Rightarrow(R\rightarrow P)\rightarrow(S\rightarrow P)$.

证法三　用形式证明

编　号	公　　式	依　据
(1)	$(P\rightarrow Q)\rightarrow R$	前提
(2)	$R\rightarrow P$	附加前提
(3)	$(P\rightarrow Q)\rightarrow P$	(1),(2);I_{13}
(4)	$\neg(\neg P\vee Q)\vee P$	(3);E_{11}
(5)	$(P\wedge\neg Q)\vee P$	(4);E_{10},E_6
(6)	P	(5);E_9
(7)	$S\rightarrow P$	(6);I_6
(8)	$(R\rightarrow P)\rightarrow(S\rightarrow P)$	(2),(7);CP

例 9-23　证明$\neg(P\leftrightarrow Q)\Leftrightarrow(P\vee Q)\wedge\neg(P\wedge Q)$

证法一　$\neg(P\leftrightarrow Q)$

$\Leftrightarrow(P\leftrightarrow\neg Q)$　　E_{16}

$\Leftrightarrow(P\rightarrow\neg Q)\wedge(\neg Q\rightarrow P)$　　E_{14}

$\Leftrightarrow(\neg P\vee\neg Q)\wedge(Q\vee P)$　　E_{11}, E_6

$\Leftrightarrow(P\vee Q)\wedge\neg(P\wedge Q)$　　E_1', E_1, E_{10}'

证法二　先证$\neg(P\leftrightarrow Q)\Rightarrow(P\vee Q)\wedge\neg(P\wedge Q)$

假定$\neg(P\leftrightarrow Q)$为真，则$P\leftrightarrow Q$为假.

(1) 若P为真，则Q为假，此时$P\vee Q$为真；$P\wedge Q$为假，所以，$\neg(P\wedge Q)$为真，因此$(P\vee Q)\wedge\neg(P\wedge Q)$为真；

(2)若P为假，则Q为真. 类似(1)可证得$(P\vee Q)\wedge\neg(P\wedge$

Q)也为真.

于是$\neg(P\leftrightarrow Q)\Rightarrow(P\vee Q)\wedge\neg(P\wedge Q)$.

下面证$(P\vee Q)\wedge\neg(P\wedge Q)\Rightarrow\neg(P\leftrightarrow Q)$

假定$\neg(P\leftrightarrow Q)$为假,则$P\leftrightarrow Q$为真.

(1) 若P为真,则Q为真,此时$P\wedge Q$为真,$\neg(P\wedge Q)$为假,所以,$(P\vee Q)\wedge\neg(P\wedge Q)$为假.

(2) 若P为假,则Q为假,此时,$P\vee Q$为假,从而$(P\vee Q)\wedge\neg(P\wedge Q)$为假.

所以$(P\vee Q)\wedge\neg(P\wedge Q)\Rightarrow\neg(P\leftrightarrow Q)$

因此$\neg(P\leftrightarrow Q)\Leftrightarrow(P\vee Q)\wedge\neg(P\wedge Q)$

注:此题用证法一较简单,给出证法二是为了开拓读者的思路,另外此题也可形式证明,参见例8-22证法三。

例9-24 设A,B,C为任意命题公式,试判断以下说法是否正确,并简单说明之.

(1) 若$A\vee C\Leftrightarrow B\vee C$,则$A\Leftrightarrow B$;

(2) 若$A\wedge C\Leftrightarrow B\wedge C$,则$A\Leftrightarrow B$;

(3) 若$A\wedge C\Rightarrow C$,则$A\Rightarrow B\rightarrow C$.

解 (1)此结论不一定成立,如令$C=P\vee\neg P$(P为命题变元),$A=P,B=\neg P$,则对任意的真值指派,$A\vee C$和$B\vee C$取值均为真,但A与B的取值正好相反,故$A\Leftrightarrow B$不成立;

(2)若有某种真值指派使A为真,C为假,B为假,则此时$A\wedge C$与$B\wedge C$的真值均为假,但A与B的真值不同,故$A\Leftrightarrow B$不一定成立;

反例,$C=P\wedge\neg P,A=P,B=\neg P$.总有$A\wedge C\Leftrightarrow B\wedge C$,但$A\Leftrightarrow B$不成立;

(3)假定公式A取值为真,若B取值为假,则$B\rightarrow C$取值为真;若B取值为真,则$A\wedge B$为真,由条件$A\wedge B\Rightarrow C$知,C为真,于是$B\rightarrow C$取值为真.所以$A\Rightarrow B\rightarrow C$,即结论成立.

例9-25 判定$(\neg P\rightarrow\neg Q)\wedge(Q\rightarrow\neg R)\wedge\neg P\Rightarrow(\neg Q\wedge$

$\neg R)$是否成立，并说明理由.

解 假定前件真，则$\neg P$，$\neg P\to\neg Q$，$Q\to\neg R$均为真，于是$\neg Q$为真，Q为假，R可取值真或假，此时，蕴含式的后件的真值依赖于R的真值取值. 当R为真时，后件$\neg Q\wedge\neg R$为假；当R为假时. 后件$\neg Q\wedge\neg R$为真. 因此，对于P,Q,R的一组真值指派$(0,0,1)$，$A=(\neg P\to\neg Q)\wedge(Q\to\neg R)\wedge\neg P$取值为1，$B=(\neg Q\wedge\neg R)$取值为0，故$A\to B$非重言式，所以$A\Rightarrow B$不成立.

例 9-26 形式证明$P\to(Q\to R),S\to Q\Rightarrow P\to(S\to R)$.

证

编 号	公 式	依 据
(1)	$P\to(Q\to R)$	前提
(2)	P	附加前提
(3)	$Q\to R$	(1),(2);I_{11}
(4)	$S\to Q$	前提
(5)	$S\to R$	(3),(4);I_{13}
(6)	$P\to(S\to R)$	(2),(5);CP规则

例 9-27 将下述推理符号化，并判断是否正确.

有红、黄、蓝、白四队参加足球联赛. 如果红队第三，则当黄队第二时，蓝队第四；或者白队不是第一，或者红队第三；事实上，黄队第二. 因此，如果白队第一，那么蓝队第四.

解 设P:红队第三；Q:黄队第二；R:蓝队第四；S:白队第一. 则上述推理符号化为$P\to(Q\to R),\neg S\vee P,Q\Rightarrow S\to R$

形式证明上述蕴含式

编 号	公 式	依 据
(1)	$\neg S\vee P$	前提
(2)	S	附加前提
(3)	P	(1),(2);I_{10}
(4)	$P\to(Q\to R)$	前提
(5)	$Q\to R$	(3),(4);I_{11}

续表

编号	公式	依据
(6)	Q	前提
(7)	R	(5),(6);I_{11}
(8)	$S \to R$	(2),(7);CP 规则

因此,上述文字推理正确.

例 9-28 小李或小张是先进工作者.如果小李是先进工作者,你是会知道的.如果小张是先进工作者,小赵也是先进工作者.你不知道小李是先进工作者,问谁是先进工作者?试利用逻辑推理来确定谁是先进工作者,并写出推理过程.

解 先将已知条件符号化.

令 P:小李是先进工作者;Q:小张是先进工作者;R:你知道小李是先进工作者;T:小赵是先进工作者.

由条件得推理的前提:$P \vee Q$、$P \to R$,$Q \to T$,$\neg R$.

下面根据已知前提进行形式推理.

编号	公式	依据
(1)	$P \to R$	前提
(2)	$\neg R$	前提
(3)	$\neg P$	(1),(2);I_{12}
(4)	$P \vee Q$	前提
(5)	Q	(3),(4);I_{10}
(6)	$Q \to T$	前提
(7)	T	(5),(6);I_{11}
(8)	$Q \wedge T$	(5),(7);I_9

因此,由上述推理知小张和小赵是先进工作者.

例 9-29 证明下式的有效性

$\neg(P\to Q)\to\neg(R\lor S),(Q\to P)\lor\neg R,R\Rightarrow P\leftrightarrow Q$

证

编　号	公　　式	依　　据
(1)	$(Q\to P)\lor\neg R$	前提
(2)	R	前提
(3)	$Q\to P$	(1),(2);I_{10}
(4)	$\neg(P\to Q)\to\neg(R\lor S)$	前提
(5)	$R\lor S$	(2);I_3
(6)	$(R\lor S)\to(P\to Q)$	(4);E_{16}
(7)	$P\to Q$	(5),(6);I_{11}
(8)	$(P\to Q)\land(Q\to P)$	(3),(7);I_9
(9)	$P\leftrightarrow Q$	(8);E_{14}

例 9-30　判断下述推理是否正确：

(1) 如果 2 是偶数，则 3 是奇数. 或者 2 是偶数或者 2 整除 3，结果 2 整除 3，所以 3 不是奇数.

(2) 一个侦探在调查了某珠宝商店的钻石项链盗窃后，根据以下事实：

a) 营业员 A 或 B 盗窃了钻石项链；

b) 若 A 作案，则作案不在营业时间；

c) 若 B 提供的证词正确，则货柜未上锁；

d) 若 B 提供的证词不正确，则作案发生在营业时间；

e) 货柜上了锁.

推断 B 盗了项链.

解　(1)先将推理过程符号化.

令 P:2 是偶数;Q:3 是奇数;R:2 整除 3.

于是，问题转化为要判断 $P\to Q,P\lor R,R\Rightarrow\neg Q$ 是否正确.

∵ $F=((P\to Q)\wedge(P\vee R)\wedge R)\to\neg Q$

$$\Leftrightarrow((\neg P\vee Q)\wedge R)\to\neg Q$$

$$\Leftrightarrow(P\wedge\neg Q)\vee\neg R\vee\neg Q$$

$$\Leftrightarrow\neg Q\vee\neg R.$$

由 F 不是重言式，知推理不正确.

(2) 将推理过程符号化：

令 P：营业员 A 盗窃了钻石项链；Q：营业员 B 盗窃了钻石项链；R：作案发生在营业时间；S：B 提供证词正确；T：货柜上了锁.

问题转化为要判断 $P\vee Q, P\to\neg R, S\to\neg T, \neg S\to R, T\Rightarrow Q$ 是否正确. 下面进行形式推理.

编号	公式	依据
(1)	$S\to\neg T$	前提
(2)	T	前提
(3)	$\neg S$	(1),(2);E_6,I_{12}
(4)	$\neg S\to R$	前提
(5)	R	(3),(4);I_{11}
(6)	$P\to\neg R$	前提
(7)	$\neg P$	(5),(6);E_6,I_{12}
(8)	$P\vee Q$	前提
(9)	Q	(7),(8);I_{10}

因此，推理判断正确.

第十章　谓词逻辑

10.1　内容提要

1. 基本论述

· 个体、谓词、量词；
· 命题函数，个体域，全总个体域，特性谓词.

2. 谓词公式的有关概念

· 原子公式(原始公式)，谓词公式；
· 量词的辖域，约束变元，自由变元；
· 换名规则，代入规则；
· 谓词公式，谓词公式的指派；
· 永真公式，永假公式，可满足公式.

3. 谓词公式间的关系

· 谓词公式间的等值关系($A\Leftrightarrow B$)；
· 谓词公式间的蕴含关系($A\Rightarrow B$)；
· 等值定律，即一些基本的等值式；
· 推理定律，即一些基本的蕴含式.

4. 谓词演算的推理理论

在谓词演算中，命题演算的推理理论仍然成立，另外还用到与量词有关的推理规则.

· 全称特定化规则(US)；

· 存在特定化规则(ES);
· 全称一般化规则(UG);
· 存在一般化规则(EG).

10.2 基本知识点

1. 谓词演算的命题符号化

个体是可以独立存在的物体,它既可以是一个具体的事物,也可以是一个抽象的概念.

谓词是用来刻划个体的性质或个体之间关系的词.

例 10-1 用个体、谓词表示下列命题

(1) 武汉位于重庆与上海之间;

(2) 如果王英坐在李红的后面,则王英比李红高.

解 (1)个体 a,b,c 分别表示武汉、重庆和上海,谓词 $P(x,y,z)$表示 x 位于 y 与 z 之间,则命题(1)可表示为 $P(a,b,c)$.

(2)令 a:王英;b:李红;$P(x,y)$:x 坐在 y 的后面;$G(x,y)$:x 比 y 高. 于是(2)可表示为

$$P(a,b)\rightarrow G(a,b).$$

量词是在命题中表示数量的词,量词有三种类型:全称量词"$\forall x$",存在量词"$\exists x$"和存在唯一量词"$\exists!x$".

由 n 元谓词 P 和 n 个个体变元 $x_1,x_2,\cdots,x_n$ 组成的表达式 $P(x_1,x_2,\cdots,x_n)$称为命题函数[1]. 命题函数中个体变元 $x_i(i=1,2,\cdots,n)$的取值范围称为 x_i 的个体域.

例 10-2 将下列命题符号化:

(1) 每个母亲都爱自己的孩子;

(2) 有某些实数是有理数;

---

[1] 本书中不严格区分 n 元谓词 $P(x_1,x_2,\cdots,x_n)$与命题函数 $P(x_1,x_2,\cdots,x_n)$.

(3) 对任何整数 x,y，若 $xy=0$，则 $x=0$ 或 $y=0$.

解 (1)令 $L(x)$：x 爱自己的孩子. x 的个体域为全体母亲组成的集合，于是(1)可表示为 $\forall xL(x)$.

(2)令 $Q(x)$：x 是有理数. x 的个体域为实数集，则(2)可表示为 $\exists xQ(x)$；

(3)令 $Z(x)$：$x=0$；$E(x,y,z)$：$x\cdot y=z$，其中 x,y,z 的个体域为整数集. 这样(3)可表示为

$$\forall x\forall y(\exists z(E(x,y,z)\wedge Z(z))\rightarrow(Z(x)\vee Z(y)).$$

需要指出的是，例 10-2 中每个命题符号化时，包含量词的表达式与个体域有关. 因此，为了准确地表达命题含义，必需用文字指明个体域，且不同的个体对应的个体域可能不同. 为了方便，将所有个体变元的个体域统一起来，引入全总个体域，即所有个体构成的个体域. 在使用全总个体域时，对个体变化的真正取值范围，用特性谓词加以限制. 一般地，对全称量词，将特性谓词作蕴含的前件；对存在量词，将特性谓词作合取项.

对例 10-2 中命题使用全总个体域，引入相应的特性谓词 $M(x)$：x 是母亲；$R(x)$：x 是实数；$I(x)$：x 是整数. 于是前面的命题可表示为：

(1) $\forall x(M(x)\rightarrow L(x))$；

(2) $\exists x(R(x)\wedge Q(x))$；

(3) $\forall x\forall y((I(x)\wedge I(y))\rightarrow\exists z((I(z)\wedge E(x,y,z)\wedge Z(z))\rightarrow(Z(x)\vee Z(y))))$.

在谓词演算中进行命题符号化时，首先确定个体域，一般使用全总个体域；然后分析命题中的个体以及各个个体间的关系，确定谓词；最后根据表示数量的词确定量词，并利用联结词将整个命题符号化.

例 10-3 将下列命题符号化(使用全总个体域).

(1) 并非每个实数都是有理数；

(2) 天下乌鸦一般黑；

(3) 任何金属都可以溶解在某种液体中；

(4) 所有人的指纹都不一样.

解 (1)该语句可理解为"有某个实数不是有理数"或"不是每个实数都是有理数."令 $R(x)$：x 是实数；$Q(x)$：x 是有理数. 则(1)可表示为 $\exists x(R(x) \wedge \neg Q(x))$ 或者 $\neg \forall x(R(x) \to Q(x))$；

(2)令 $W(x)$：x 是乌鸦；$B(x,y)$：x 与 y 一样黑；则(2)可表示为 $\forall x \forall y((W(x) \wedge W(y)) \to B(x,y))$；

(3)令 $J(x)$：x 是金属；$E(x)$：x 是液体；$S(x,y)$：x 可以溶解于 y 中. 则(3)可以表示为 $\forall x(J(x) \to \exists y(E(y) \wedge S(x,y)))$；

(4)令 $M(x)$：x 是人；$N(x,y)$：x 不是 y；$Q(x,y)$：x 与 y 的指纹一样. 则(4)可以表示为 $\forall x \forall y((M(x) \wedge M(y) \wedge N(x,y)) \to \neg Q(x,y))$. 或者表示为：$\neg \exists x \exists y(M(x) \wedge M(y) \wedge N(x,y) \wedge Q(x,y))$.

例 10-4 在数学分析中函数 $f(x)$ 在点 a 连续的定义为：对任意的 $\varepsilon > 0$，存在一个 $\delta > 0$，使得对所有 x，若 $|x-a| < \delta$，则 $|f(x) - f(a)| < \varepsilon$，把上述定义符号化.

解 令 $R(x)$：x 是实数；$G(x,y)$：x 大于 y.

$\forall \varepsilon((R(\varepsilon) \wedge G(\varepsilon,0)) \to \exists \delta(R(\delta) \wedge G(\delta,0) \wedge \forall x((R(x) \wedge G(\delta,|x-a|)) \to G(\varepsilon,|f(x)-f(a)|))))$.

例 10-5 设 x,y 的个体域为自然数集合，定义其中的原子公式如下：$P(x)$：x 是素数；$E(x)$：x 是偶数；$O(x)$：x 是奇数；$D(x,y)$：x 可以整除 y. 试将下列各式译成自然语言：

(1) $\exists x(E(x) \wedge D(x,6))$；

(2) $\forall x(O(x) \to \forall y(P(x) \to \neg D(x,y))$.

解 (1)有某个偶数能整除 6.

(2)任何奇数不能整除每个素数.

2. 谓词公式和变元的约束

我们将命题常量 0、1，一个命题和命题变元以及一个命题函

数 $P(x_1, x_2, \cdots, x_n)$ 统称为原子公式. 由原子公式、联结词和量词可构成谓词公式其定义为

(1)原子公式是谓词公式;

(2)如果 A、B 是谓词公式,则 $\neg A$, $(A \vee B)$, $(A \wedge B)$, $(A \to B)$, $(A \leftrightarrow B)$ 也是谓词公式;

(3)如果 A 是谓词公式, x 是 A 中的自由变元,则 $\forall xA$ 和 $\exists xA$ 也是谓词公式;

(4)只有经过有限次使用上述三条规则而得到的才是谓词公式. 简称公式.

前面例 10-1—例 10-4 所符号化的表达式均是谓词公式.

例 10-6 将下列语句用谓词公式符号化:

(1) 每个人的祖母都是他父亲的母亲;

(2) 对于每一个实数 x,存在一个更大的实数 y;

(3) 没有一位女同志既是国家选手又是家庭妇女;

(4) 如果明天天气好,有些学生将去公园.

解 (1)令 $P(x)$: x 是人; $G(x,y)$: x 是 y 的祖母; $F(x,y)$: y 是 x 的父亲; $M(x,y)$: y 是 x 的母亲. 则该语句可表示为

$$\forall x \forall y((P(x) \wedge P(y) \wedge G(y,x)) \to \exists z(P(z) \wedge F(x,z) \wedge M(z,y))).$$

(2)令 $R(x)$: x 是实数; $G(x,y)$: x 比 y 大,则该语句可表示为

$$\forall x(R(x) \to \exists y(R(y) \wedge G(y,x))).$$

(3)令 $W(x)$: x 是一位女同志; $C(x)$: x 是国家选手; $H(x)$: x 是家庭妇女. 这样该语句可表示为

$$\neg \exists x(W(x) \wedge C(x) \wedge H(x)).$$

(4)令 H: 明天天气好; $S(x)$: x 是学生; $P(x)$: x 是公园; $Q(x,y)$: x 去 y 处. 这样该语句可表示为

$$H \to \exists x(S(x) \wedge \exists y(P(y) \wedge Q(x,y))).$$

在公式 F 中,形如 $\forall xA(x)$ 或 $\exists xA(x)$ 的子公式称为公式 F 的 x 约束部分, $A(x)$ 称为相应量词的辖域, x 在辖域中的出现,称

为 x 在公式 F 中的约束出现. 所有约束出现的变元,称为约束变元. 在公式 F 中,x 的非约束出现,称为 x 在公式 F 中的自由出现,自由出现的变元称为自由变元.

例 10-7 指出下列表达式中的自由变元和约束变元,并指明量词的辖域.

(1) $\forall x(P(x,y) \wedge \exists yQ(y)) \wedge (\forall xR(x) \to Q(x))$;

(2) $\forall x(P(x,y) \vee Q(z)) \wedge \exists y(R(x,y) \to \forall zQ(z))$.

解 (1)$\forall x$ 的辖域为 $P(x,y) \wedge \exists yQ(y)$,$\exists y$ 的辖域为 $Q(y)$,第二个$\forall x$ 的辖域为 $R(x)$. 在(1)式中,x 既是约束变元,又是自由变元. 因为 x 在 $Q(x)$中是自由出现,而在 $P(x,y)$中却是约束出现. y 是约束变元.

(2) $\forall x$ 的辖域为 $P(x,y) \vee Q(z)$,$\exists y$ 的辖域为 $R(x,y) \to \forall zQ(z)$,$\forall z$ 的辖域为 $Q(z)$. 在(2)式中,x,y,z 均既是约束变元,又是自由变元. 这是因为 x 在 $P(x,y)$中是约束出现,但在 $R(x,y)$中是自由出现;y 在 $P(x,y)$中是自由出现,但在 $R(x,y)$中是约束出现;z 在第一个 $Q(z)$中是自由出现,但在第二个 $Q(z)$中是约束出现.

3. 变元的换名和代人

对约束变元换名时,必须将该变元在量词及其辖域中的所有出现都同时换名为该辖域中未出现过的符号,最好是公式中未出现过的符号.

例 10-8 对公式$\forall x(P(x,y) \wedge \exists yQ(y) \wedge M(x,y)) \wedge (\forall xR(x) \to Q(x))$中的约束变元进行换名,使每个变元在公式中只呈一种出现形式(即约束出现或自由出现).

解 在该公式中,将 $P(x,y)$和 $M(x,y)$中的约束变元 x 换名为 z,$R(x)$中的 x 换名为 v,$Q(y)$中的 y 换名为 u,换名后为

$$\forall z(P(z,y) \wedge \exists uQ(u) \wedge M(z,y))$$
$$\wedge (\forall vR(v) \to Q(x)).$$

注意 若将公式换名为$\forall z(P(z,y)\wedge\exists uQ(u)\wedge M(x,y))\wedge(\forall vR(v)\rightarrow Q(x))$则是错误的，因为它未将$\forall x$辖域$(P(x,y)\wedge\exists yQ(y)\wedge M(x,y))$中$x$的所有出现同时换名.

对公式中的自由变元代入时，必须对该自由变元在公式中的所有自由出现同时进行代入，并且代入时所选用的符号不在原公式中出现.

例 10-9 对公式$(\exists yA(x,y)\rightarrow(\forall xB(x,z)\wedge C(x,y,z)))\wedge\exists x\forall zC(x,y,z)$中的自由变元进行代入，使每个变元在公式中只是一种出现形式.

解 将该公式中的自由变元x用t代入，y用u代入，z用v代入，代入后为

$$(\exists yA(t,y)\rightarrow(\forall xB(x,v)\wedge C(t,u,v)))\wedge\exists x\forall zC(x,u,z).$$

注意 (1)若将公式代入成

$$(\exists yA(t,y)\rightarrow(\forall xB(x,z)\wedge C(x,u,v)))\wedge\exists x\forall zC(x,u,z),$$

则是错误的，因为这一代入过程未将公式中x和z的所有自由出现同时进行代入；

(2) 若将公式代入成

$$(\exists yA(t,y)\rightarrow(\forall xB(x,x)\wedge C(t,x,v))\wedge\exists x\forall zC(x,x,z)$$

也是错误的. 在代入过程中选用了公式中约束出现的变元符号，改变了原公式的含义.

4. 公式的指派及公式的类型

由于谓词公式包含命题变元和命题函数，不能确定其真值，故不是命题，但若一个谓词公式不含命题变元且命题函数中的个体变元均被约束，那么该公式的真值是确定的，它就是一个命题.

例 10-10 令$S(x,y,z)$表示$x+y=z$；$P(x,y,z)$表示$x\cdot y$

$=z$；$L(x,y)$表示$x<y$，x,y的个体域为非负整数集，用以上所设的原子谓词公式表示下列语句，并判断各谓词公式是否为命题，是命题的指出其真值.

(1) 没有x小于0；

(2) 有某个y，对所有的x使得$x+y=y$；

(3) 存在着x，使得$x\cdot y=y$对所有的y成立；

(4) 任意x满足$x<y$.

解 (1)符号化为$\neg\exists xL(x,0)$或$\forall x(\neg L(x,0))$. 该公式是真命题；

(2) 符号化为$\exists y\forall xS(x,y,y)$，由于$x,y$均被约束，故$\exists y\forall xS(x,y,y)$是命题，而$1+y\neq y$，故是假命题；

(3) 符号化为$\exists x\forall yP(x,y,y)$，因为$1\cdot y=y$，故该公式是真命题；

(4) 符号化为$\forall xL(x,y)$，由于在命题函数$L(x,y)$中变元y未被约束，故在个体域中$\forall xL(x,y)$的真值不确定，所以$\forall xL(x,y)$不是命题.

设D是一个非空个体域，若n元谓词P和n个个体变元$x_1,x_2,\cdots,x_n$组成的命题函数$P(x_1,x_2,\cdots,x_n)$，对D中任一有序n元组$(a_1,a_2,\cdots,a_n)$都有确定的真假值，则称P为个体域D上的谓词. 若公式F中的所有谓词均是D上的谓词，则称公式F的个体域为D. 设F是谓词公式，D是F的非空个体域. 若对公式F中的每个自由个体变元都用D中确定的个体代入，命题变元用确定的命题或真值(0或1)代入，公式F就有了确定的真值，从而变成了命题，这样一组代入到公式F中的确定的个体、命题或真值(0或1)称为公式F的一组指派.

永真公式：如果对公式F的任意一组指派均使F为真，则称F为永真公式.

永假公式：如果对公式F的任意一组指派均使F为假，则称F为永假公式.

可满足公式：如果至少有一组指派使公式 F 为真，则称 A 是可满足公式.

例 10-11 对公式 $F=\exists x(P(x)\wedge Q(x,y))\vee R$ 给出二个指派，分别使公式取值为真和假，其中 $P(x)$ 表示"x 是偶数"，$Q(x,y)$ 表示"y 能整除 x."F 的个体域 $D=\{3,4\}$，R 是命题变元.

解 指派：$y=4$，R 为 1，则因为 $P(4)$ 为 1，$Q(4,4)$ 为 1，所以 $\exists x(P(x)\wedge Q(x,y))$ 为 1，又 R 为 1，因此 F 对此指派取值为 1.

再指派：R 为 0，$y=3$.

若 $x=4$，则 $P(4)$ 为 1，但 $Q(4,3)$ 为 0；

若 $x=3$，则 $P(3)$ 为 0，$Q(3,3)$ 为 1.

对此指派 $\exists x(P(x)\wedge Q(x,y))$ 总为 0，又 R 被指派为 0，所以，F 对该指派取值为 0.

例 10-12 判定下列公式的类型：

(1) $\forall x\exists yG(x-y,x+y)\wedge(Q\vee\neg Q)$；

(2) $G(x-y,x+y)$；

(3) $\forall x\forall y(G(x,y)\wedge\neg G(x,y))\wedge Q$.

其中 x,y 的个体域为整数集 I，Q 为命题变元，$G(x,y)$ 表示 $x<y$.

解 (1) 无论对 Q 指派何种命题常元，$Q\vee\neg Q$ 的真值总为 1，而在 I 中对任意的 x，总存在 $y=1$ 使 $x-1<x+1$ 成立，所以命题 $\forall x\exists yG(x-y,x+y)$ 在 I 中总为真，因此 $\forall x\exists yG(x-y,x+y)\wedge(Q\wedge\neg Q)$ 对任意的指派总为真，是永真公式.

(2) 因为 $x-y<x+y$ 在 I 中的真值不确定，当指派 $x=1,y=1$ 时，$0<2$，即 $x-y<x+y$ 取值为真；当指派 $x=4,y=-1$ 时，$5<3$ 不成立，即 $x-y<x+y$ 取值为假，所以，公式 $G(x-y,x+y)$ 是可满足公式.

(3) 无论给 x,y 指派什么个体，$G(x,y)\wedge\neg G(x,y)$ 总为假，从而 $\forall x\forall y(G(x,y)\wedge\neg G(x,y))\wedge Q$ 总为假，所以该公式为永假公式.

5. 谓词公式的等值式

设 A、B 是两个具有共同个体域 E 的公式，若对于 A 和 B 的任意一组指派，公式 A 和 B 都有相同的真值，即 $A \leftrightarrow B$ 是永真公式，则称公式 A 和 B 在 E 上等值，记作 $A \Leftrightarrow B$，称 $A \Leftrightarrow B$ 为等值式. 亦即 A 与 B 间有等值关系.

当个体域是有限集合时，原则上来说，可以用真值表的方法来验证一个公式是否为永真公式，或者验证两个公式是否等值. 但是，当个体域的元素或公式中的命题变元的个数较多时，用真值表方法判定等值式显然是不可行的，于是一般用等值演算的方法证明. 命题演算中的基本等值式都可推广到谓词演算中使用，此外还有如表 10-2 所列的等值式.

例 10-13 判定等值式 $(\exists xQ(x,y) \vee R) \Leftrightarrow \forall x(\neg Q(x,y)) \rightarrow R$ 是否成立，其中 x,y 的个体域为 $D=\{3,4\}$，R 为命题变元，$Q(x,y)$ 表示 x 能整除 y.

解 列出两个公式相对各种可能指派的如表 10-1 所示.

表 10-1

$x\ y\ R$	$Q(x,y)$	$\exists xQ(x,y)$	$\forall x(\neg Q(x,y))$	$\exists xQ(x,y) \vee R$	$\forall x(\neg Q(x,y)) \rightarrow R$
3 3 1	1	1	0	1	1
3 4 1	0	1	0	1	1
4 3 1	0	1	0	1	1
4 4 1	1	1	0	1	1
3 3 0	1	1	0	1	1
3 4 0	0	1	0	1	1
4 3 0	0	1	0	1	1
4 4 0	1	1	0	1	1

注意　当 $y=3$ 时，$\because Q(3,3)\Leftrightarrow 1$，$\therefore \exists xQ(x,y)\Leftrightarrow 1$，而 $\forall x(\neg Q(x,3))\Leftrightarrow \neg Q(3,3)\wedge \neg Q(4,3)\Leftrightarrow 0\wedge 1\Leftrightarrow 0$

当 $y=4$ 时，$\because Q(4,4)\Leftrightarrow 1$，$\therefore \exists xQ(x,y)\Leftrightarrow 1$，而 $\forall x(\neg Q(x,4))\Leftrightarrow \neg Q(3,4)\wedge \neg Q(4,4)\Leftrightarrow 1\wedge 0\Leftrightarrow 0$ 因此，由表 10-1 知等值式 $(\exists xQ(x,y)\vee R)\Leftrightarrow \forall x(\neg Q(x,y))\rightarrow R$ 成立，且公式 $A=\exists xQ(x,y)\vee R$ 和公式 $B=\forall x(\neg Q(x,y))\rightarrow R$ 本身都是永真公式

E_{18}　$\neg(\forall xA(x))\Leftrightarrow \exists x(\neg A(x))$
E_{19}　$\neg(\exists xA(x))\Leftrightarrow \forall x(\neg A(x))$
（E_{18}、E_{19}：量词转换律）

E_{20}　$\forall x(A(x)\wedge B)\Leftrightarrow \forall xA(x)\wedge B$
E_{21}　$\forall x(A(x)\vee B)\Leftrightarrow \forall xA(x)\vee B$
E_{22}　$\exists x(A(x)\wedge B)\Leftrightarrow \exists xA(x)\wedge B$
E_{23}　$\exists x(A(x)\vee B)\Leftrightarrow \exists xA(x)\vee B$
（E_{20}—E_{23}：量词辖域的扩张与收缩律）

E_{24}　$\forall x(A(x)\wedge B(x))\Leftrightarrow \forall xA(x)\wedge \forall xB(x)$
E_{25}　$\exists x(A(x)\vee B(x))\Leftrightarrow \exists xA(x)\vee \exists xB(x)$
（E_{24}、E_{25}：量词分配律）

E_{26}　$\exists x(A(x)\rightarrow B)\Leftrightarrow \forall xA(x)\rightarrow B$

E_{27}　$\forall x(A(x)\rightarrow B)\Leftrightarrow \exists xA(x)\rightarrow B$

E_{28}　$\exists x(A\rightarrow B(x))\Leftrightarrow A\rightarrow \exists xB(x)$

E_{29}　$\forall x(A\rightarrow B(x))\Leftrightarrow A\rightarrow \forall xB(x)$

E_{30}　$\exists x(A(x)\rightarrow B(x))\Leftrightarrow \forall xA(x)\rightarrow \exists xB(x)$

上各式中的 B 表示任意一个不含有约束变元 x 的公式.

例 10-14　证明下列等值式

(1) $\forall xA(x)\wedge \forall x(\neg B(x))\Leftrightarrow \neg \exists x(A(x)\rightarrow B(x))$;

(2) $\forall x\forall y(P(x)\rightarrow Q(y))\Leftrightarrow (\exists xP(x)\rightarrow \forall yQ(y))$.

分析　同证明命题演算中的等值式一样，证明两个公式等值时，可以从其中任一公式开始进行演算，一般从较复杂的公式开始，另外，还可以对两个公式 F_1 和 F_2 分别进行等值演算，如果能将公式 F_1 和 F_2 都等值演算为同一公式 F_3，那么由等值关系的传递性，即可知 $F_1\Leftrightarrow F_2$.

证(1) $\because \neg\exists x(A(x)\rightarrow B(x))$

$\Leftrightarrow\forall x\neg(A(x)\rightarrow B(x))$　　E_{19}

$\Leftrightarrow\forall x\neg(\neg A(x)\vee B(x))$　　E_{11}

$\Leftrightarrow\forall x(A(x)\wedge\neg B(x))$　　E_{10}

$\Leftrightarrow\forall xA(x)\wedge\forall x(\neg B(x))$　　E_{24}

$\therefore\forall xA(x)\wedge\forall x(\neg B(x))\Leftrightarrow\neg\exists x(A(x)\neg B(x))$.

(2) $\because\forall x\forall y(p(x)\rightarrow Q(y))$

$\Leftrightarrow\forall x\forall y(\neg p(x)\vee Q(y))$　　E_{11}

$\Leftrightarrow\forall x(\forall yQ(y)\vee\neg p(x))$　　E_1,E_{21}

$\Leftrightarrow\forall x(\neg p(x))\vee\forall yQ(y)$　　E_1,E_{21}

$\Leftrightarrow\neg\exists xp(x)\vee\forall yQ(y)$　　E_{19}

$\Leftrightarrow\exists xp(x)\rightarrow\forall yQ(y)$　　E_{11}

$\therefore\forall x\forall y(P(x)\rightarrow Q(y))\Rightarrow(\exists xP(x)\rightarrow\forall yQ(y))$

注意　$P(x)$中不含约束变元y,$Q(y)$中不含约束变元x,故可使用E_{21}.

例 10-15　判定下列公式哪些是永真式,对所得结论进行论证.

(1) $\forall x(A(x)\rightarrow B(x))\rightarrow(\exists xA(x)\rightarrow\exists xB(x))$;

(2) $(\forall xA(x)\rightarrow\forall xB(x))\rightarrow\forall x(A(x)\rightarrow B(x))$.

解　(1) $\because\forall x(A(x)\rightarrow B(x))\rightarrow(\exists xA(x)\rightarrow\exists xB(x))$

$\Leftrightarrow\neg\forall x(\neg A(x)\vee B(x))\vee(\neg\exists xA(x)\vee\exists xB(x))$

E_{11}

$\Leftrightarrow\exists x\neg(\neg A(x)\vee B(x))\vee\exists xB(x)\vee\neg\exists xA(x)$

E_{18},E_1

$\Leftrightarrow\exists x(A(x)\wedge\neg B(x))\vee\exists xB(x)\vee\neg\exists xA(x)$

E_{10},E_2

$\Leftrightarrow\exists x((A(x)\wedge\neg B(x))\vee B(x))\vee\neg\exists xA(x)$

E_{25}

$\Leftrightarrow\exists x(A(x)\vee B(x))\vee\neg\exists xA(x)$　　E_3,E_5,E_4'

$\Leftrightarrow \exists xA(x) \vee \exists xB(x) \vee \neg \exists xA(x)$　　　E_{25}

$\Leftrightarrow (\exists xA(x) \vee \neg \exists xA(x)) \vee \exists xB(x)$　　　E_1, E_3

$\Leftrightarrow 1$.

$\therefore \forall x(A(x) \to B(x)) \to (\exists xA(x) \to \exists xB(x))$是永真式.

(2) 此公式不是永真式. 若假定 x 的个体域是实数集 R. $A(x)$: x 是有理数; $B(x)$: x 是整数. 则$\forall xA(x)$和$\forall xB(x)$均为假,于是$\forall xA(x) \to \forall xB(x)$为真. 又因为$\forall x(A(x) \to B(x))$为假($\because$ 有理数不一定是整数). 因此$(\forall xA(x) \to \forall xB(x)) \to \forall x(A(x) \to B(x))$为假.

6. 谓词公式的蕴含式

设 A, B 是两个具有共同个体域 E 的公式,若 $A \to B$ 是永真公式,即 $A \to B \Leftrightarrow 1$,则称公式 A 蕴含公式 B,记作 $A \Rightarrow B$,称 $A \Rightarrow B$ 为蕴含式,亦即 A 与 B 间有蕴含关系.

谓词公式蕴含式 $A \Rightarrow B$ 的判定方法:

(1)由等值演算证明 $A \to B \Leftrightarrow 1$;

(2)由基本等值式和基本蕴含式推导出 $A \Rightarrow B$;

(3)假定前件 A 为真,检查在此情况下,其后件 B 是否也为真;

(4)假定后件为假,检查在此情况下,其前件 A 是否也假.

常用的基本蕴含式如表 10-2 所示:

表 10-2

I_{15}	$\exists x(A(x) \wedge B(x)) \Rightarrow \exists xA(x) \wedge \exists xB(x)$	量词分配蕴含律
I_{16}	$\forall xA(x) \vee \forall xB(x) \Rightarrow \forall x(A(x) \vee B(x))$	
I_{17}	$\forall x(A(x) \to B(x)) \Rightarrow \forall xA(x) \to \forall xB(x)$	

例 10-16　判定下列蕴含式是否成立.

(1) $\exists x \exists y(P(x) \wedge Q(y)) \Rightarrow \exists xP(x)$;

(2) $(\exists xP(x)\to\forall xQ(x))\Rightarrow\forall x(P(x)\to Q(x))$；

(3) $\forall x(P(x)\vee Q(x))\Rightarrow\forall xp(x)\vee\exists xQ(x)$.

证 (1) $\because \exists x\exists y(P(x)\wedge Q(y))\to\exists xP(x)$

$\Leftrightarrow\exists x(P(x)\wedge\exists yQ(y))\to\exists xP(x)$ $\qquad E_{22}$

$\Leftrightarrow\neg(\exists xP(x)\wedge\exists yQ(y))\vee\exists xP(x)$ $\qquad E_{22},E_{11}$

$\Leftrightarrow\neg\exists xP(x)\vee\neg\exists yQ(y)\vee\exists xP(x)$ $\qquad E_{10}$

$\Leftrightarrow(\neg\exists xP(x)\vee\exists xP(x))\vee\neg\exists yQ(y)$ $\qquad E_1,E_3$

$\Leftrightarrow 1$ $\qquad E_5,E_8$

$\therefore\exists x\exists y(P(x)\wedge Q(y))\Rightarrow\exists xP(x)$.

注意 $\because P(x)$中不含约束变元y,$Q(y)$中不含约束变元x,
$\therefore$在第一步和第二步可使用E_{22}.

(2) $\because(\exists xP(x)\to\forall xQ(x))$

$\Leftrightarrow\neg\exists xP(x)\vee\forall xQ(x)$ $\qquad E_{11}$

$\Leftrightarrow\forall x\neg P(x)\vee\forall xQ(x)$ $\qquad E_{19}$

$\Rightarrow\forall x(\neg P(x)\vee Q(x))$ $\qquad I_{16}$

$\Leftrightarrow\forall x(P(x)\to Q(x))$ $\qquad E_{11}$

$\therefore\exists xP(x)\to\forall xQ(x)\Rightarrow\forall x(P(x)\to Q(x))$.

(3) **方法一** 假定前件$\forall x(P(x)\vee Q(x))$为真,则对每个x_0,$P(x_0)\vee Q(x_0)$为真.若对某个x_0,$Q(x_0)$为真,则$\exists xQ(x)$为真,从而后件$\forall xP(x)\vee\exists xQ(x)$也为真;若对每个$x_0$,$Q(x_0)$均为假,由于$P(x_0)\vee Q(x_0)$总为真,故一定是对每个$x_0$,$P(x_0)$均为真,即$\forall xP(x)$为真.所以后件$\forall xP(x)\vee\exists xQ(x)$为真.

方法二 假定后件$\forall xP(x)\vee\exists xQ(x)$为假,则$\forall xP(x)$为假,且$\exists xQ(x)$也为假.即存在某个$x_0$使$Q(x_0)$为假,对任意的$x_1$,$P(x_1)$均为假,于是$P(x_0)\vee Q(x_0)$为假,因此$\forall x(P(x)\vee Q(x))$为假,所以

$$\forall x(P(x)\vee Q(x))\Rightarrow\forall xP(x)\vee\exists xQ(x).$$

7. 多个量词间的次序关系

多个量词连续出现,它们之间无括号分隔时,后面的量词在前

面量词的辖域之中，且量词对变元的约束与量词的次序有关，一般不能随意调动，但也有例外，两个量词间的排列次序有如下常用公式

E_{31}　$\forall x\forall yA(x,y)\Leftrightarrow\forall x\forall yA(x,y)$

E_{32}　$\exists x\exists yA(x,y)\Leftrightarrow\exists y\exists xA(x,y)$

I_{18}　$\forall x\forall yA(x,y)\Rightarrow\exists y\forall xA(x,y)$

I_{19}　$\forall x\exists yA(x,y)\Rightarrow\exists y\exists xA(x,y)$

I_{20}　$\exists y\forall xA(x,y)\Rightarrow\forall x\exists yA(x,y)$

注意　由 E_{31} 和 E_{32} 知相同量词的次序可以任意调动.

例 10-17　下列蕴含关系是否成立？若成立，给出证明，否则给出反例.

(1) $\exists xA(x)\rightarrow B\Rightarrow\forall xA(x)\rightarrow B$;

(2) $\forall x\exists yP(x,y)\Rightarrow\exists y\forall xp(x,y)$.

解　(1)假定后件假，即 $\forall xA(x)\rightarrow B$ 为假，则 $\forall xA(x)$ 为真，B 为假，于是 $\exists xA(x)$ 也为真，从而 $\exists xA(x)\rightarrow B$ 为假，所以，$\exists xA(x)\rightarrow B\Rightarrow\forall xA(x)\rightarrow B$.

(2) 此蕴含式不成立.

反例，设 x,y 的个体域均为自然数集 N，$P(x,y)$：$x<y$. 因为，对任何 x，总有 $y=x+1$，使 $P(x,y)$ 为真，所以，$\forall x\exists yP(x,y)$ 为真. 但是在 N 中不存在一个 y_0，使得对任意的 x 均有 $x<y$，如 $x_1=y_0+1$，就不满足 $P(x_1,y_0)$，从而 $\exists y\forall xP(x,y)$ 为假，因此蕴含式不成立.

8. 谓词演算的推理理论

在谓词演算中，命题演算的推理理论仍然成立. 另外还要用到下面四条推理规则.

i) US(全称特定化规则)

$\forall xA(x)\Rightarrow A(y)$.

此规则成立的条件是：

(1) x 是 $A(x)$中的自由变元；

(2) y 在 $A(x)$中不约束出现，最好 $A(x)$中不含 y；

(3) 自由变元 y，可以写成个体域中任意一个个体常元 c. 即 $\forall xA(x) \Rightarrow A(c)$.

ii) ES(存在特定化规则)

$\exists xA(x) \Rightarrow A(c)$.

此规则成立的条件是：

(1) c 是个体域中某个确定的个体；

(2) c 不曾在 $A(x)$中出现过；

(3) 若 $A(x)$中还有其他自由变元出现，则 x 不能随其他自由变元变化.

iii) UG(全称一般化规则)

$$A(x) \Rightarrow \forall yA(y)$$

此规则成立的条件是：

(1) x 在 $A(x)$中自由出现，且 x 取个体域中任何值时，$A(x)$均为真；

(2) 代替 x 的 y 不能在 $A(x)$中约束出现.

iv) EG(存在一般化规则)

$$A(c) \Rightarrow \exists yA(y).$$

此规则成立的条件是：

(1) c 是个体域中某个确定的个体；

(2) 代替 c 的 y 不能在 $A(c)$中出现过.

例 10-18 判断下述推理过程是否正确，并说明理由.

i)

编　号	公　　式	依　　据
(1)	$\forall x \exists y(x>y)$	前提
(2)	$\exists y(z>y)$	(1)；US
(3)	$z>c$	(2)；ES

续表

编　号	公　　式	依　　据
(4)	$\forall x(x>c)$	(3);UG
(5)	$c>c$	(4);US
(6)	$\forall x(x>x)$	(5);UG

ii) 证明$\exists xP(x)\land\exists xQ(x)\Rightarrow\exists x(P(x)\land Q(x))$.

编　号	公　　式	依　　据
(1)	$\exists xp(x)\land\exists xQ(x)$	前提
(2)	$\exists xp(x)$	(1);I_1
(3)	$\exists xQ(x)$	(2);I_2
(4)	$P(c)$	(2);ES
(5)	$Q(c)$	(3);ES
(6)	$P(c)\land Q(c)$	(4),(5);I_9
(7)	$\exists x(P(x)\land Q(x))$	(6);EG

解　i)推理过程不正确.

当x,y的个体域为整数集时,$\forall x\exists y(x>y)$为真,却推出了假命题$\forall x(x>x)$. 其出错原因是在(3)步不能使用ES规则,因为$A(y)$为$(z>y)$中y随自由变元z而变化,不满足ES要求的条件(3),所以造成推导过程出错.

ii) 推理过程不正确

若x的个体域为整数集,$P(x)$:x是奇数;$Q(x)$:x是偶数,则由真命题$\exists xP(x)\land\exists xQ(x)$,推出了假命题$\exists x(P(x)\land Q(x))$. 其出错原因是在(4)、(5)步使用$ES$时,同时选用了$c$,此处在(5)步上只能用$d$,且$d$与$c$不一定相同.

例 10-19 形式证明下述各蕴含式

i) $\neg\exists x(p(x)\wedge Q(a)),\exists xp(x)\Rightarrow\neg Q(a)$;

ii) $\forall x(p(x)\rightarrow(Q(y)\wedge R(x))),\exists xp(x)\Rightarrow Q(y)\wedge\exists x(p(x)\wedge R(x))$;

iii) $\forall x(F(x)\rightarrow\neg G(x)),\forall x(G(x)\vee H(x)),\exists x(\neg H(x))\Rightarrow\exists x(\neg F(x))$.

分析 由于 US,ES 规则中量词前均无联结词"$\neg$",因此,若含量词的公式前有"$\neg$",可利用 E_{18}和 E_{19}替换.

证 i)

编 号	公 式	依 据
(1)	$\neg\exists x(P(x)\wedge Q(a))$	前提
(2)	$\forall x(\neg(P(x)\wedge Q(a)))$	(1);$E_{.9}$
(3)	$\exists xP(x)$	前提
(4)	$P(c)$	(3);ES
(5)	$\neg(P(c)\wedge Q(a))$	(2);US
(6)	$\neg P(c)\vee\neg Q(a)$	(5);E_{10}
(7)	$\neg Q(a)$	(4),(6);I_{10}

注意 (4),(5)步不能颠倒,即若要同时使用 US 和 ES 规则,应先使用 ES 规则,后使用 US 规则,若反过来,就只能得 $\neg(P(d)\wedge Q(a))$,此处不能保证 $d=c$.

ii)

编 号	公 式	依 据
(1)	$\forall x(P(x)\rightarrow(Q(y)\wedge R(x)))$	前提
(2)	$\exists xP(x)$	前提
(3)	$P(c)$	(2);ES

续表

编　号	公　　式	依　　据
(4)	$P(c)\to(Q(y)\wedge R(c))$	(1);US
(5)	$Q(y)\wedge R(c)$	(3),(4);I_{11}
(6)	$Q(y)$	(5);I_1
(7)	$R(c)$	(5);I_2
(8)	$P(c)\wedge R(c)$	(3),(7);I_9
(9)	$\exists x(P(x)\wedge R(x))$	(8);EG
(10)	$Q(y)\wedge\exists x(P(x)\wedge R(x))$	(6),(9);I_9

iii)

编　号	公　　式	依　　据
(1)	$\exists x(\neg H(x))$	前提
(2)	$\forall x(G(x)\vee H(x))$	前提
(3)	$\neg H(c)$	(1);ES
(4)	$G(c)\vee H(c)$	(2);US
(5)	$G(c)$	(3),(4);I_9
(6)	$\forall x(F(x)\to\neg G(x))$	前提
(7)	$F(c)\to\neg G(c)$	(6);US
(8)	$\neg F(c)$	(5),(7);I_{12}
(9)	$\exists x\neg F(x)$	(8);EG

使用 US,ES,UG,EG 这四条规则时,要注意严格按照它们所要求的条件去使用,并且从整体上考虑个体变元和常元符号的选择. 尤其对 EG 和 ES 规则的应用,要避免选择已在证明序列前面公式中出现过的符号进行取代. 另外这四条规则中量词的辖域应

包括整个公式，且它们都是蕴含式，因此，不能对某个公式的部分，应用这四个规则中的任何一个，这样可能会引出错误.

9. 间接证法

当根据前提集进行推导，无从着手时，可采用间接证法，即反证法，把结论的否定作为附加前提，这样好像多了一个条件，推演起来方便些. 但任何事情都不是绝对的，要视情况而定.

例 10-20 用形式证明的方法证明

i) $\exists xA(x)\rightarrow\forall xB(x)\Rightarrow\forall x(A(x)\rightarrow B(x))$;

ii) $\forall x(P(x)\rightarrow\neg Q(x)),\forall x(Q(x)\vee R(x)),\exists x\neg R(x)\Rightarrow\exists x\neg P(x)$

证 i)

编 号	公 式	依 据
(1)	$\exists xA(x)\rightarrow\forall xB(x)$	前提
(2)	$\neg\forall x(A(x)\rightarrow B(x))$	附加前提
(3)	$\exists x\neg(A(x)\rightarrow B(x))$	(2);E_{18}
(4)	$\neg(A(c)\rightarrow B(c))$	(3);ES
(5)	$A(c)\wedge\neg B(c)$	(4);E_{11},E_{10}
(6)	$A(c)$	(5);I_1
(7)	$\exists xA(x)$	(6);EG
(8)	$\forall xB(x)$	(7),(1);I_{11}
(9)	$B(c)$	(8);US
(10)	$\neg B(c)$	(5);I_2
(11)	$B(c)\wedge\neg B(c)$	(9),(10);I_9(矛盾)

$\therefore\exists xA(x)\rightarrow\forall xB(x)\Rightarrow\forall x(A(x)\rightarrow B(x))$.

说明： 若第(7)步不是将 $A(c)$使用 EG 规则得到$\exists xA(x)$，

而是由(1)$\exists xA(x)\rightarrow\forall xB(x)$，使用 ES 得 $A(c)\rightarrow\forall xB(x)$后，也能推出结论，但这样推演是错误的，因为它对部分公式使用 ES 规则，而且在使用 ES 规则时，选用了前面序列已选用过的个体 c.

证 ii) **方法一**

编号	公式	依据
(1)	$\forall x(P(x)\rightarrow\neg Q(x))$	前提
(2)	$\neg\exists x\neg P(x)$	附加前提
(3)	$\forall xP(x)$	(1);E_{19}
(4)	$\forall x(Q(x)\vee R(x))$	前提
(5)	$\exists x\neg R(x)$	前提
(6)	$\neg R(c)$	(5);ES
(7)	$Q(c)\vee R(c)$	(4);US
(8)	$Q(c)$	(6),(7);I_{10}
(9)	$P(c)$	(3);US
(10)	$P(c)\rightarrow\neg Q(c)$	(1);US
(11)	$\neg Q(c)$	(9),(10);I_{11}
(12)	$Q(c)\wedge\neg Q(c)$	(8),(11);I_9(矛盾)

$\therefore \forall x(P(x)\rightarrow\neg Q(x)),\forall x(Q(x)\vee R(x)),\exists x\neg R(x)\Rightarrow\exists x\neg P(x)$.

说明 1)上述推理过程中，必须先对(5)中$\exists x\neg R(x)$使用 ES，然后再对(1),(3),(4)中的公式使用 US，否则不能保证特定化个体的一致性；

2) i)小题不用间接证法，不好着手推演，但 ii)小题不用间接证法还可简化几步.

方法二

编号	公式	依据
(1)	$\forall x(Q(x)\vee R(x))$	前提
(2)	$\exists x\neg R(x)$	前提
(3)	$\neg R(c)$	(2);ES
(4)	$Q(c)\vee R(c)$	(1);US
(5)	$Q(c)$	(3),(4);I_{10}
(6)	$\forall x(P(x)\rightarrow\neg Q(x))$	前提
(7)	$P(c)\rightarrow\neg Q(c)$	(6);US
(8)	$\neg P(c)$	(5),(7);I_{12}
(9)	$\exists x\neg P(x)$	(8);EG

10. 前束范式

一个谓词公式，如果它的所有量词均出现在公式的开头，且它们的辖域一直延伸到公式的末尾，则称此种形式的公式为前束范式.

前束范式可记作下述形式：

$$Q_1x_1Q_2x_2\cdots Q_kx_kB,$$

其中，每个 $Q_i(1\leqslant i\leqslant k)$为量词$\forall$ 或$\exists$ ，x_i 是个体变元，B 为不含量词的谓词公式.

若一个谓词公式 A 具有如下形式：

$Q_1x_1Q_2x_2\cdots Q_kx_k(A_{11}\vee A_{12}\vee\cdots\vee A_{1n_1})\wedge\cdots\wedge(A_{m1}\vee A_{m2}\vee\cdots\vee A_{mn_m})$

则称 A 为前束合取范式；

若 A 具有如下形式：

$Q_1x_1Q_2x_2\cdots Q_kx_k(A_{11}\wedge A_{12}\wedge\cdots\wedge A_{1n_1})\vee\cdots\vee(A_{m1}\wedge\cdots\wedge A_{mn_m})$

则称 A 为前束析取范式. 其中 A_{ij}是原子谓词公式或其否定,Q_i 和 x_i 的含义同上.

每个谓词公式 A 均可以变换为与它等值的前束合取范式和前束析取范式. 其步骤如下:

(1) 消去联结词$\rightarrow$,$\leftrightarrow$;

(2) 将联结词$\neg$向内深入,使之只作用于原子谓词公式;

(3) 利用换名或代入规则使所有约束变元的符号均不同,并且自由变元与约束变元的符号也不同;

(4) 利用量词辖域的扩张和收缩律,扩大量词的辖域至整个公式;

(5) 利用分配律将公式化为前束合取范式或前束析取范式.

例 10-21 将公式 A:

$\forall x(A(x)\rightarrow B(x,y))\rightarrow(\exists yC(y)\rightarrow\exists zD(y,z))$化为前束合取范式.

解 (1)消去联结词$\rightarrow$和$\leftrightarrow$:

$$A\Leftrightarrow\neg\forall x(\neg A(x)\vee B(x,y))\vee(\neg\exists yC(y)\vee\exists zD(y,z)) \quad E_{11}$$

(2) 将联结词$\neg$深入至原子公式

$$A\Leftrightarrow\exists x\neg(\neg A(x)\vee B(x,y))\vee(\forall y\neg C(y)\vee\exists zD(y,z)) \quad E_{18},E_{19}$$

$$\Leftrightarrow\exists x(A(x)\wedge\neg B(x,y))\vee(\forall y\neg C(y)\vee\exists zD(y,z)) \quad E_{10}$$

(3) 换名

$$A\Leftrightarrow\exists x(A(x)\wedge\neg B(x,y))\vee(\forall t\neg C(t)\vee\exists zD(y,z))$$

(4) 将量词提到整个公式的前面

$$A\Leftrightarrow\exists x(A(x)\wedge\neg B(x,y))\vee\forall t\exists z(\neg C(t)\vee D(y,z)) \quad E_{23},E_{21}$$

$$\Leftrightarrow\exists x\forall t\exists z((A(x)\wedge\neg B(x,y))\vee\neg C(t)\vee D(y,z)) \quad E_{23},E_{21}$$

至此，已得到 A 的前束范式.

(5) 利用分配律将其化为前束合取范式

$A \Leftrightarrow \exists x \forall t \exists z((A(x) \vee \neg C(t) \vee D(y,z)) \wedge (\neg B(x,y) \vee \neg C(t) \vee D(y,z)))$.

例 10-22 求等值于公式 $B=(\exists xP(x) \vee \exists xQ(x)) \rightarrow \exists x(P(x) \vee Q(x))$的前束析取范式

解 $B \Leftrightarrow \neg(\exists xP(x) \vee \exists xQ(x)) \vee \exists x(P(x) \vee Q(x))$ $\quad E_{11}$

$\Leftrightarrow (\neg\exists xP(x) \wedge \neg\exists xQ(x)) \vee \exists x(P(x) \vee Q(x))$ $\quad E_{10}$

$\Leftrightarrow (\forall x\neg P(x) \wedge \forall x\neg Q(x)) \vee \exists x(P(x) \vee Q(x))$ $\quad E_{19}$

$\Leftrightarrow \forall x(\neg P(x) \wedge \neg Q(x)) \vee \exists x(P(x) \vee Q(x))$ $\quad E_{24}$

$\Leftrightarrow \forall x(\neg P(x) \wedge \neg Q(x)) \vee \exists y(P(y) \vee Q(y))$ 换名规则

$\Leftrightarrow \forall x \exists y((\neg P(x) \wedge \neg Q(x)) \vee P(y) \vee Q(y))$ $\quad E_{23}$

10.3 问答与论证

例 10-23 判断下列推证是否正确，说明理由.

证明$\forall x(P(x) \vee Q(x)) \Rightarrow \forall xP(x) \vee \forall xQ(x)$.

证明过程为

$\because \forall x(P(x) \vee Q(x))$

$\Leftrightarrow \neg\exists x\neg(P(x) \vee Q(x))$ $\quad E_6, E_{18}$

$\Leftrightarrow \neg\exists x(\neg P(x) \wedge \neg Q(x))$ $\quad E_{10}$

$\Rightarrow \neg(\exists x\neg P(x) \wedge \exists x\neg Q(x))$ $\quad I_{15}$

$\Leftrightarrow \neg\exists x\neg P(x) \vee \neg\exists x\neg Q(x)$ $\quad I_{10}$

$\Leftrightarrow \forall xP(x) \vee \forall xQ(x)$ $\quad E_{18}, E_6$

$\therefore \forall x(P(x) \vee Q(x)) \Rightarrow \forall xP(x) \vee \forall xQ(x)$.

解 此推证是错误的，在推导的第三步，错误地应用了 I_{15}，因为$\neg\exists x(\neg P(x) \wedge \neg Q(x))$与 I_{15}的前件相比多了“$\neg$”联结词，在第九章例 9-14 中说明若 $A \Leftrightarrow B$，则$\neg A \Leftrightarrow \neg B$；若 $A \Rightarrow B$，却不一定

$\neg A \Rightarrow \neg B$. 所以，在第三步不能使用 I_{15}. 下面的反例说明蕴含式不成立.

令 $P(x)$：x 是奇数；$Q(x)$：x 是偶数. x 的个体域为整数集. 则 $\forall x(P(x) \vee Q(x))$ 总真，但 $\forall xP(x)$ 和 $\forall xQ(x)$ 均假，因此蕴含式不成立.

例 10-24 下述推理是否正确，若不正确，请指出其推理过程中的错误.

i)

编　号	公　　式	依　　据
(1)	$\exists x(A(x) \rightarrow B(x))$	前提
(2)	$\exists xA(x)$	附加前提
(3)	$A(c)$	(2)；ES
(4)	$A(c) \rightarrow B(c)$	(1)；ES
(5)	$B(c)$	(3)，(4)；I_{11}
(6)	$\exists xB(x)$	(5)；EG

$\therefore \exists x(A(x) \rightarrow B(x)) \Rightarrow \exists xA(x) \rightarrow \exists xB(x)$.

ii)

编　号	公　　式	依　　据
(1)	$\forall x(A(x) \rightarrow B(x))$	前提
(2)	$\forall xA(x) \rightarrow \forall xB(x)$	(1)；I_{17}
(3)	$A(c) \rightarrow \forall xB(x)$	(2)；US
(4)	$\exists xA(x) \rightarrow \forall xB(x)$	(3)；EG

$\therefore \forall x(A(x) \rightarrow B(x)) \Rightarrow \exists xA(x) \rightarrow \forall xB(x)$.

解 i)推理不正确.

若 x 的个体域为自然数集 N，$A(x)$：x 是奇数；$B(x)$：$x<0$，则$\exists x(A(x)\rightarrow B(x))$为真，（如 $2\in N$，$A(2)$假，$A(2)\rightarrow B(2)$为真）却推出了假命题$\exists xA(x)\rightarrow\exists xB(x)$（其前件真，后件总假.）其出错原因是在(3)步已引入个体常元 c，而在第(4)应用 ES 规则时，又引入个体常元 c，结果由真前件，推出了假命题.

ii）推理不正确

若 x 的个体域为实数集 R，$A(x)$：x 是整数；$B(x)$：x 是有理数. 则$\forall x(A(x)\rightarrow B(x))$为真，$\exists xA(x)$也为真，但$\forall xB(x)$为假，于是$\exists xA(x)\rightarrow\forall xB(x)$为假. 即由真前件推出了假命题. 其出错原因是在(3)，(4)步对部分公式错误地使用规则 US 和 EG.

例 10-25 证明下列各式

i）$\forall x(P(x)\vee Q(x)),\forall x(Q(x)\rightarrow\neg R(x))\Rightarrow\forall xR(x)\rightarrow\forall xP(x)$；

ii）$\forall x((P(x)\wedge Q(x))\rightarrow\exists y(R(y)\wedge S(x,y)))\Rightarrow\neg\exists yR(y)\rightarrow\neg\exists x(P(x)\wedge Q(x))$.

分析 由于命题演算中的推理理论在谓词演算中均成立，故此类结论为蕴含形式表达式的形式证明，通常采用蕴含规则，即 CP 规则.

证 i）

编　号	公　　式	依　　据
(1)	$\forall xR(x)$	附加前提
(2)	$\forall x(Q(x)\rightarrow\neg R(x))$	前提
(3)	$R(c)$	(1)；US
(4)	$Q(c)\rightarrow\neg R(c)$	(2)；US
(5)	$\neg Q(c)$	(3)，(4)；I_{12}
(6)	$\forall x(P(x)\vee Q(x))$	前提
(7)	$P(c)\vee Q(c)$	(6)；US
(8)	$P(c)$	(5)，(7)；I_{10}
(9)	$\forall xP(x)$	(8)；UG
(10)	$\forall xR(x)\rightarrow\forall xP(x)$	(1)，(9)；CP

ii) **方法一**

编　号	公　　式	依　　据
(1)	$\neg\exists yR(y)$	附加前提
(2)	$\forall y\neg R(y)$	(1);E_{19}
(3)	$\forall x((P(x)\land Q(x))\to\exists y(R(y)\land S(x,y)))$	前提
(4)	$(P(c)\land Q(c))\to\exists y(R(y)\land S(c,y))$	(3);US
(5)	$\neg(P(c)\land Q(c))\lor\exists y(R(y)\land S(c,y))$	(4);E_{11}
(6)	$\exists y(\neg(P(c)\land Q(c))\lor(R(y)\land S(c,y)))$	(5);E_{23}
(7)	$\neg(P(c)\land Q(c))\lor(R(d)\land S(c,d))$	(6);ES
(8)	$\neg R(d)$	(2);US
(9)	$\neg R(d)\lor\neg S(c,d)$	(8);I_3
(10)	$\neg(R(d)\land S(c,d))$	(9);E_{10}
(11)	$\neg(P(c)\land Q(c))$	(7),(10);I_{10}
(12)	$\forall x\neg(P(x)\land Q(x))$	(11);UG
(13)	$\neg\exists x(P(x)\land Q(x))$	(12);E_{19}
(14)	$\neg\exists yR(y)\to\neg\exists x(P(x)\land Q(x))$	(1),(13);CP

说明　(1)不能直接对(4)中的公式使用 ES，因为那样是将对部分公式使用 ES 规则；

(2)不是对任意的个体变元均能使用 UG 规则，这里(11)中的 c 原本是在(4)步用 US 规则得到的，即它对个体域中的每个个体均成立，所以在(12)步可以使用 UG 规则.

(3)若将此题的结论先作一等值变换，可使推理过程简化.

方法二

$\because \neg\exists yR(y)\to\neg\exists x(P(x)\land Q(x))$

$\Leftrightarrow \exists x(p(x) \wedge Q(x)) \to \exists yR(y) \qquad E_{15}$

∴原命题转化为证明

$\forall x((p(x) \wedge Q(x)) \to \exists y(R(y) \wedge S(x,y)))$

$\Rightarrow \exists x(p(x) \wedge Q(x)) \to \exists yR(y)$.

编 号	公 式	依 据
(1)	$\exists x(P(x) \wedge Q(x))$	附加前提
(2)	$P(c) \wedge Q(c)$	(1);ES
(3)	$\forall x((p(x) \wedge Q(x)) \to \exists y(R(y) \wedge S(x,y)))$	前提
(4)	$(P(c) \wedge Q(c)) \to \exists y(R(y) \wedge S(c,y))$	(3);US
(5)	$\exists y(R(y) \wedge S(c,y))$	(2),(4);I_{11}
(6)	$\exists yR(y) \wedge \exists yS(c,y)$	(5);I_{15}
(7)	$\exists yR(y)$	(6);I_1
(8)	$\exists x(p(x) \wedge Q(x)) \to \exists yR(y)$	(1),(7);CP
(9)	$\neg\exists yR(y) \to \neg\exists x(p(x) \wedge Q(x))$	(8);E_{15}

例 10-26 符号化下列命题并推证其结论：

(1)没有不守信用的人是可以信赖的，有些可以信赖的人是受过教育的人，因此，有些受过教育的人是守信用的；

(2)每个运动员都是强壮的. 每一个既强壮又聪明的人都将在事业中获得成功. 吴平是运动员，并且是聪明的. 因此，吴平一定能在事业中获得成功；

(3)如果一个人长期吸烟或酗酒，那么他身体绝不会健康. 如果一个人身体不健康，那么他就不能参加体育比赛. 有人参加了体育比赛，所以有人不长期酗酒；

(4)每一个买到门票的人，都能得到座位. 因此，如果这里已没有座位，那么就没有任何人买到门票.

解 (1)先将命题符号化，设个体域是人的集合.

令 $M(x)$：x 是守信用的；$J(x)$：x 受过教育；$D(x)$：x 可以信赖.

前提：$\neg\exists x(\neg M(x)\wedge D(x))$，$(\exists x(D(x)\wedge J(x))$ 有效结论：$\exists x(J(x)\wedge M(x))$.

证

编　号	公　　式	依　　据
(1)	$\neg\exists x(\neg M(x)\wedge D(x))$	前提
(2)	$\forall x\neg(\neg M(x)\wedge D(x))$	(1)；E_{15}
(3)	$\exists x(D(x)\wedge J(x))$	前提
(4)	$D(c)\wedge J(c)$	(3)；ES
(5)	$\neg(\neg M(c)\wedge D(c))$	(2)；US
(6)	$M(c)\vee\neg D(c)$	(5)；E_{10}
(7)	$D(c)$	(4)；I_1
(8)	$M(c)$	(6)，(7)；I_{10}
(9)	$J(c)$	(4)；I_2
(10)	$J(c)\wedge M(c)$	(8)，(9)；I_9
(11)	$\exists x(J(x)\wedge M(x))$	(10)；EG

(2)设个体域为人的集合

令 $P(x)$：x 是运动员；$Q(x)$：x 强壮；$R(x)$：x 聪明；$S(x)$：x 在事业中成功；a：吴平.

将命题符合化为

$$\forall x(P(x)\rightarrow Q(x)),\forall x((Q(x)\wedge R(x))\rightarrow S(x)),P(a)\wedge R(a)\Rightarrow S(a).$$

也可设个体域为全总个体域，令 $M(x)$：x 是人. 则命题符号化为

$$\forall x((M(x)\wedge P(x))\rightarrow Q(x)),\forall x((M(x)\wedge Q(x)\wedge R(x))\rightarrow S(x)),M(a)\wedge P(a)\wedge R(a)\Rightarrow S(a).$$

证

编 号	公 式	依 据
(1)	$M(a)\land P(a)\land R(a)$	前提
(2)	$\forall x((M(x)\land P(x))\rightarrow Q(x))$	前提
(3)	$(M(a)\land P(a))\rightarrow Q(a)$	(2);US
(4)	$M(a)\land P(a)$	(1);E_2';I_1
(5)	$Q(a)$	(3),(4);I_{11}
(6)	$\forall x((M(x)\land Q(x)\land R(x))\rightarrow S(x))$	前提
(7)	$(M(a)\land Q(a)\land R(a))\rightarrow S(a)$	(6);US
(8)	$M(a)\land R(a)$	(1);E_1',E_2',I_1
(9)	$M(a)\land Q(a)\land R(a)$	(5),(8);I_9,E_1',E_2'
(10)	$S(a)$	(7),(9);I_{11}

(3) 设个体域为全总个体域

令 $M(x)$:x 是人,$C(x)$:x 长期吸烟;$K(x)$:x 长期酗酒;$J(x)$:x身体健康;$P(x)$:x 能参加体育比赛.

则命题符号化为

$$\forall x((M(x)\land(C(x)\lor K(x)))\rightarrow\neg J(x)),$$
$$\forall x((M(x)\land\neg J(x))\rightarrow\neg P(x)),$$
$$\exists x(M(x)\land P(x))\Rightarrow\exists x(M(x)\land\neg K(x)).$$

证

编 号	公 式	依 据
(1)	$\exists x(M(x)\land P(x))$	前提
(2)	$M(c)\land P(c)$	(1);ES
(3)	$\forall x((M(x)\land\neg J(x))\rightarrow\neg P(x))$	前提

编　号	公　　式	依　　据
(4)	$(M(c)\wedge\neg J(c))\to\neg P(c)$	(3);US
(5)	$P(c)$	(2);I_2
(6)	$\neg(M(c)\wedge\neg J(c))$	(4),(5);I_{12}
(7)	$\neg M(c)\vee J(c)$	(6);E_{10}
(8)	$M(c)$	(2);I_1
(9)	$J(c)$	(7),(8);I_{10}
(10)	$\forall x((M(x)\wedge(C(x)\vee K(x)))\to\neg J(x))$	前提
(11)	$(M(c)\wedge(C(c)\vee K(c)))\to\neg J(c)$	(10);US
(12)	$\neg(M(c)\wedge(C(c)\vee K(c)))$	(9),(11);I_{12}
(13)	$\neg M(c)\vee(\neg C(c)\wedge\neg K(c))$	(12);E_{10},E_{10}'
(14)	$\neg C(c)\wedge\neg K(c)$	(8),(13);I_{10}
(15)	$\neg K(c)$	(14);I_2
(16)	$M(c)\wedge\neg K(c)$	(8),(15);I_9
(17)	$\exists x(M(x)\wedge\neg K(x))$	(16),EG

(4)设个体域为全总个体域

令 $M(x)$:x 是人;$K(x)$:x 买到门票;$E(y)$:y 是座位;$S(x,y)$:x能得到 y. 命题符号化为:

$$\forall x((M(x)\wedge K(x))\to\exists y(E(y)\wedge S(x,y))\Rightarrow$$
$$\neg\exists yE(y)\to\neg\exists x(M(x)\wedge K(x)).$$

证 ∵ $\neg\exists yE(y)\to\neg\exists x(M(x)\wedge K(x))\Leftrightarrow$

$$\exists x(M(x)\wedge K(x))\to\exists yE(y)\qquad E_{16}$$

∴利用等值替换转化为证明.

$\forall x((M(x)\wedge K(x))\to\exists y(E(y)\wedge S(x,y)))\Rightarrow\exists x(M(x)$

$\wedge K(x))\rightarrow\exists yE(y)$.

编 号	公 式	依 据
(1)	$\exists x(M(x)\wedge K(x))$	前提
(2)	$M(c)\wedge K(c)$	(1);ES
(3)	$\forall x((M(x)\wedge K(x))\rightarrow\exists y(E(y)\wedge S(x,y)))$	前提
(4)	$(M(c)\wedge K(c))\rightarrow\exists y(E(y)\wedge S(c,y))$	(3);US
(5)	$\exists y(E(y)\wedge S(c,y))$	(2),(4);I_{11}
(6)	$\exists yE(y)\wedge\exists yS(c,y)$	(5);I_{15}
(7)	$\exists yE(y)$	(6);I_1
(8)	$\exists x(M(x)\wedge K(x))\rightarrow\exists yE(y)$	(1),(7);CP
(9)	$\neg\exists yE(y)\rightarrow\neg\exists x(M(x)\wedge K(x))$	(8);E_{16}

例 10-27 用构造推理过程的方法证明

$\exists xF(x),\exists x(R(x)\wedge\neg T(x)),\forall z((F(z)\wedge\forall x\exists yQ(x,y))\rightarrow\forall y(R(y)\rightarrow T(y)))\Rightarrow\forall y\exists x\neg Q(x,y)$.

证

编 号	公 式	依 据
(1)	$\exists xF(x)$	前提
(2)	$F(c)$	(1);ES
(3)	$\exists x(R(x)\wedge\neg T(x))$	前提
(4)	$R(d)\wedge\neg T(d)$	(3);ES
(5)	$\neg(\neg R(d)\vee T(d))$	(4);E_{10}
(6)	$\neg(R(d)\rightarrow T(d))$	(5);E_{11}
(7)	$\exists y\neg(R(y)\rightarrow T(y))$	(6);EG
(8)	$\neg\forall y(R(y)\rightarrow T(y))$	(7);E_8

续表

编号	公式	依据
(9)	$\forall z((F(z)\wedge\forall x\exists yQ(x,y))\rightarrow\forall y(R(y)\rightarrow T(y)))$	前提
(10)	$(F(c)\wedge\forall x\exists yQ(x,y))\rightarrow\forall y(R(y)\rightarrow T(y))$	(9);US
(11)	$\neg(F(c)\wedge\forall x\exists yQ(x,y))$	(8),(10);I_{12}
(12)	$\neg F(c)\vee\neg\forall x\exists yQ(x,y)$	(11);E_{10}
(13)	$\neg\forall x\exists yQ(x,y)$	(2),(12);I_{10}
(14)	$\exists x\neg(\exists yQ(x,y))$	(13);E_{18}
(15)	$\neg\exists yQ(e,y)$	(14);ES
(16)	$\forall y\neg Q(e,y)$	(15);E_{19}
(17)	$\exists x\forall y\neg Q(x,y)$	(16);EG
(18)	$\forall y\exists x\neg Q(x,y)$	(17);I_{20}

例 10-28 设命题函数 $R_A(x)$:x 属于实数集合 A;$R_B(x)$:x 属于实数集合 B;$G(x,y)$:$x>y$.

试将命题“并非 A 中的数都不比 B 中的数大”按下列要求分别用谓词公式表示.

(1)只出现全称量词;

(2)只出现存在量词;

(3)量词全部放在公式的前部.

解 (1)$\neg\forall x(R_A(x)\rightarrow\forall y(R_B(y)\rightarrow\neg G(x,y)))$

(2)$\exists x(R_A(x)\wedge\exists y(R_B(y)\wedge G(x,y)))$

可以验证(1)$\Leftrightarrow$(2)

$\neg\forall x(R_A(x)\rightarrow\forall y(R_B(y)\rightarrow\neg G(x,y)))$

$\Leftrightarrow\exists x\neg(\neg R_A(x)\vee\forall y(\neg R_B(y)\vee\neg G(x,y)))$　　E_{18},E_{11}

$\Leftrightarrow\exists x(R_A(x)\wedge\neg\forall y\neg(R_B(y)\wedge G(x,y)))$　　E_{10}

$\Leftrightarrow\exists x(R_A(x)\wedge\exists y(R_B(y)\wedge G(x,y)))$　　E_{18}

(3)$\exists x\exists y(R_A(x)\wedge R_B(y)\wedge G(x,y))$

D. 解题思路与方法

例 D-1 在一次亚洲女排比赛中，赛前有甲、乙、丙三人对这次比赛结果分别作了如下的预测：

甲：日本第一，韩国第三；

乙：中国第一，日本第三；

丙：韩国第一，日本第二.

比赛结束后发现三个人都恰好预测对一个，问中、韩、日三国女排在这次比赛中的名次如何排列？（假定无并列名次）.

分析 这类分析判定问题，首先是将条件符号化，然后可用等值演算的方法解决.

解 设 P_i, Q_i, R_i 分别表示中国第 i 名，韩国第 i 名，日本第 i 名($i=1,2,3$)，显然 P_i, Q_i, R_i 中均有一个真命题.

由于甲、乙、丙三人都恰好预测对一个，故有等值式：

(1) $(R_1 \land \neg Q_3) \lor (\neg R_1 \land Q_3) \Leftrightarrow 1$;

(2) $(P_1 \land \neg R_3) \lor (\neg P_1 \land R_3) \Leftrightarrow 1$;

(3) $(Q_1 \land \neg R_2) \lor (\neg Q_1 \land R_2) \Leftrightarrow 1$.

因为重言式的合取仍为重言式，所以(1) $\land$ (2) $\Leftrightarrow 1$. 即 $1 \Leftrightarrow [(R_1 \land \neg Q_3) \lor (\neg R_1 \land Q_3)] \land [(P_1 \land \neg R_3) \lor (\neg P_1 \land R_3)] \Leftrightarrow (R_1 \land \neg Q_3 \land P_1 \land \neg R_3) \lor (\neg R_1 \land Q_3 \land P_1 \land \neg R_3) \lor (R_1 \land \neg Q_3 \land \neg P_1 \land R_3) \lor (\neg R_1 \land Q_3 \land \neg P_1 \land R_3)$.

由于中国和日本不能并列第一名，日本不能既第一，又第三，所以

$$(R_1 \land \neg Q_3 \land P_1 \land \neg R_3) \Leftrightarrow 0;$$

$$(R_1 \land \neg Q_3 \land \neg P_1 \land R_3) \Leftrightarrow 0,$$

于是得

(4) $(\neg R_1 \land Q_3 \land P_1 \land \neg R_3) \lor (\neg R_1 \land Q_3 \land \neg P_1 \land R_3) \Leftrightarrow 1$

再将(3)与(4)合取得

$1 \Leftrightarrow [(Q_1 \wedge \neg R_2) \vee (\neg Q_1 \wedge R_2)] \wedge [(\neg R_1 \wedge Q_3 \wedge P_1 \wedge \neg R_3) \vee (\neg R_1 \wedge Q_3 \wedge \neg P_1 \wedge R_3)] \Leftrightarrow (Q_1 \wedge \neg R_2 \wedge \neg R_1 \wedge Q_3 \wedge P_1 \wedge \neg R_3) \vee (\neg Q_1 \wedge R_2 \wedge \neg R_1 \wedge Q_3 \wedge P_1 \wedge \neg R_3) \vee (Q_1 \wedge \neg R_2 \wedge \neg R_1 \wedge Q_3 \wedge \neg P_1 \wedge R_3) \vee (\neg Q_1 \wedge R_2 \wedge \neg R_1 \wedge Q_3 \wedge \neg P_1 \wedge R_3)$.

因为中国队与韩国不能并列第一，韩国队与日本不能并列第三，日本队不能既第二，又第三. 所以

$$(Q_1 \wedge \neg R_2 \wedge \neg R_1 \wedge Q_3 \wedge P_1 \wedge \neg R_3) \Leftrightarrow 0;$$

$$(Q_1 \wedge \neg R_2 \wedge \neg R_1 \wedge Q_3 \wedge \neg P_1 \wedge R_3) \Leftrightarrow 0;$$

$$(\neg Q_1 \wedge R_2 \wedge \neg R_1 \wedge Q_3 \wedge \neg P_1 \wedge R_3) \Leftrightarrow 0.$$

于是可得(5)$(\neg Q_1 \wedge R_2 \wedge \neg R_1 \wedge Q_3 \wedge P_1 \wedge \neg R_3) \Leftrightarrow 1$.

因此 P_1, R_2, Q_3 为真，即中国第一，日本第二，韩国第三.

例 D-2 张三说李四在说谎，李四说王五在说谎，王五说张三、李四都在说谎. 问张三，李四，王五三人到底谁说真话，谁说假话?

分析 首先将命题符号化，然后利用形式证明的方法进行推演，推出的有效结论，就是我们的判定结果.

解 设 P:张三说真话；Q:李四说真话；R:王五说真话. 则依题意可得前提：

$P \to \neg Q, \neg P \to Q, Q \to \neg R, \neg Q \to R, R \to \neg P \wedge \neg Q, \neg R \to P \vee Q$.

下面根据已知前提进行形式推理

编　号	公　　式	依　　据
(1)	$P \to \neg Q$	前提
(2)	$\neg Q \to R$	前提
(3)	$P \to R$	(1),(2);I_{13}
(4)	$R \to (\neg P \wedge \neg Q)$	前提
(5)	$P \to (\neg P \wedge \neg Q)$	(3),(4);I_{13}

续表

编　号	公　　式	依　　据
(6)	$\neg P \vee (\neg P \wedge \neg Q)$	(5);E_{11}
(7)	$\neg P$	(6);E_9
(8)	$\neg P \rightarrow Q$	前提
(9)	Q	(7),(8);I_{11}
(10)	$Q \rightarrow \neg R$	前提
(11)	$\neg R$	(9),(10);I_{11}
(12)	$\neg P \wedge Q \wedge \neg R$	(7),(9),(11);I_9

因此,由上述推导知张三说假话,王五说假话,只有李四说真话.

例 D-3　对甲、乙、丙三个人进行一次智力测验,将他们排成纵队.甲在前,乙次之,丙在最后,在他们看不见的情况下给他们每人戴上一顶帽子,他们只知道帽子是从三顶红帽子和两顶黑帽子中任意选取的.现在丙能看见乙和甲的帽子,乙只能看见甲的帽子,甲不能看见任何人的帽子.测验者先问丙能否判断自己的帽子的颜色.丙回答不能.再问乙能否判断自己帽子的颜色.乙也回答不能.结果甲根据他们的回答断定自己戴的帽子是红的(不是黑色的).试给出甲的推理过程.

解　令 P_i 分别表示甲、乙、丙的帽子是黑色,Q_i 分别表示甲、乙、丙能推出自己的帽子颜色,其中 $i=1,2,3$.

甲的推理可分成下面三个层次.

(1) 根据只有两顶黑帽子的事实知 $P_1 \wedge P_2 \Rightarrow Q_3$;

(2) 考虑乙的推理依据.

乙知道丙不能判定自己的帽子颜色,且 $P_1 \wedge P_2 \Rightarrow Q_3$,于是乙可推出 $\neg Q_3, P_1 \wedge P_2 \rightarrow Q_3 \Rightarrow \neg(P_1 \wedge P_2)$,即甲与乙中至少有一人戴红帽子,若乙看见甲戴黑帽子,就一定能断定自己戴红帽子.

$P_1 \wedge P_2 \rightarrow Q_3, \neg Q_3, P_1 \Rightarrow Q_2$.

(3) 根据丙和乙的回答，甲可推出下述前提：

$P_1 \wedge P_2 \rightarrow Q_3, \neg Q_3, P_1 \rightarrow Q_2, \neg Q_2$

下面根据已知前提进行形式推理

编　号	公　式	依　据
(1)	$P_1 \rightarrow Q_2$	前提
(2)	$\neg Q_2$	前提
(3)	$\neg P_1$	(1),(2);I_{11}

所以，甲断定自己戴的不是黑帽子，故是红帽子.

例 D-4　判定下面的文字推理是否正确.

(1)“每个科学工作者都是勤奋的. 每个既勤奋又聪明的人在他的事业中都将获得成功. 王大志是科学工作者并且是聪明的，所以王大志在他的事业中将获得成功.”

(2)“有些人喜欢所有的花，但人们不喜欢杂草. 所以花不是杂草”.

解　(1)将命题符号化

令 $M(x)$: x 是人；$K(x)$: x 是科学工作者；$Q(x)$: x 勤奋；$T(x)$: x 聪明；$S(x)$: x 将获得成功；a: 王大志.

前提：$\forall x((M(x) \wedge K(x)) \rightarrow Q(x)), \forall x((M(x) \wedge Q(x) \wedge T(x)) \rightarrow S(x)), M(a) \wedge K(a) \wedge T(a)$.

结论：$S(a)$

下面根据前提进行推演

编　号	公　式	依　据
(1)	$\forall x((M(x) \wedge K(x)) \rightarrow Q(x))$	前提
(2)	$M(a) \wedge K(a) \wedge T(a)$	前提
(3)	$M(a) \wedge K(a)$	(2);E_2,I_1
(4)	$(M(a) \wedge K(a)) \rightarrow Q(a)$	(1);US

续表

编号	公式	依据
(5)	$Q(a)$	(3),(4);I_{11}
(6)	$M(a)\wedge T(a)$	(2);E_1E_2,I_1
(7)	$M(a)\wedge Q(a)\wedge T(a)$	(5),(6);I_9,E_1
(8)	$\forall x((M(x)\wedge Q(x)\wedge T(x))\rightarrow S(x))$	前提
(9)	$M(a)\wedge Q(a)\wedge T(a)\rightarrow S(a)$	(8);US
(10)	$S(a)$	(7),(9);I_{11}

因此,文字推理正确.

(2)将命题符号化

令$M(x)$:x是人;$H(x)$:x是花;$Z(x)$:x是杂草;

$K(x,y)$:x喜欢y.

前提:$\exists x(M(x)\wedge\forall y(H(y)\rightarrow K(x,y)))$,

$\forall x(M(x)\rightarrow\forall y(Z(y)\rightarrow\neg K(x,y)))$,

结论:$\forall x(H(x)\rightarrow\neg Z(x))$.

下面根据前提进行推演

编号	公式	依据
(1)	$\exists x(M(x)\wedge\forall y(H(y)\rightarrow K(x,y)))$	前提
(2)	$\forall x(M(x)\rightarrow\forall y(Z(y)\rightarrow\neg K(x,y)))$	前提
(3)	$M(c)\wedge\forall y(H(y)\rightarrow K(c,y))$	(1);US
(4)	$M(c)$	(3);I_1
(5)	$\forall y(H(y)\rightarrow K(c,y))$	(4);I_2
(6)	$M(c)\rightarrow\forall y(Z(y)\rightarrow\neg K(c,y))$	(2);US
(7)	$\forall y(Z(y)\rightarrow\neg K(c,y))$	(4),(6);I_{11}
(8)	$H(a)\rightarrow\neg K(c,a)$	(5);US

续表

编　号	公　　式	依　　据
(9)	$Z(a)\rightarrow\neg K(c,a)$	(7);US
(10)	$K(c,a)\rightarrow\neg Z(a)$	(9);E_{15}
(11)	$H(a)\rightarrow\neg Z(a)$	(8),(10);I_{13}
(12)	$\forall x(H(x)\rightarrow\neg Z(x))$	(11);UG

因此,文字推理正确.

参考文献

[1] 洪帆主编.离散数学基础(第二版).武汉:华中理工大学出版社,1995.

[2] 左孝凌,李为鉴,刘永才.离散数学.上海:上海科学技术文献出版社,1982.

[3] 耿素云,屈婉玲.离散数学基础.北京:北京大学出版社,1994.

[4] 方世昌.离散数学.西安:西北电讯工程学院出版社,1985.

[5] 马振华.离散数学导引.北京:清华大学出版社,1993.

[6] 朱洪,胡美琛,张霭珠,赵一鸣.离散数学教程.上海:上海科学技术文献出版社,1996.